Entanglement cost of implementing controlled-unitary operations

Akihito Soeda,[1,2] Peter S. Turner,[1] and Mio Murao[1,3]

[1]*Graduate School of Science, the University of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo, Japan.*
[2]*Centre for Quantum Technologies, National University of Singapore,*
3 Science Drive 2, 117543 Singapore, Singapore.
[3]*Institute for Nano Quantum Information Electronics,*
the University of Tokyo, 4-6-1, Komaba, Meguro-ku, Tokyo, Japan.
(Dated: October 28, 2011)

We investigate the minimum entanglement cost of the deterministic implementation of two-qubit controlled-unitary operations using local operations and classical communication (LOCC). We show that any such operation can be implemented by a three-turn LOCC protocol, which requires at least 1 ebit of entanglement when the resource is given by a bipartite entangled state with Schmidt number 2. Our result implies that there is a gap between the minimum entanglement cost and the entangling power of controlled-unitary operations. This gap arises due to the requirement of implementing the operations while oblivious to the identity of the inputs.

The theoretical cost of a quantum computation sets the minimum experimental resource requirements for realizing that quantum computation in practice. Entanglement cost is one important resource that needs to be minimized, especially in distributed quantum computation [1], where global unitary operations are implemented by local (quantum) operations and classical communication (LOCC) [2] assisted by entanglement.

Generally, *entanglement-assisted LOCC implementation* of an operation involves a quantum system consisting of two parts, namely an *input system* and a *resource system*. The input system may start in an arbitrary *unknown* state representing quantum information. On the other hand, the resource system is set to a particular known state that may depend on the unitary operation to be implemented, but not on the input quantum information. We take "LOCC implementation" to imply "deterministic entanglement-assisted LOCC implementation" in the rest of this Letter.

The amount of entanglement E of the resource system is called the *minimum entanglement cost* of LOCC implementation of a *unitary* operation U if the following two properties hold, (i) LOCC implementation is feasible using an entangled state with E, and (ii) LOCC implementation of U is infeasible for any resource state with less than E. Property (i) guarantees that E is an upper bound on the minimum entanglement cost, which can be proved by providing an explicit construction of the implementation protocol. On the other hand, property (ii) guarantees that E is the corresponding lower bound, and proving it is considerably more difficult, because one must show that the implementation fails for *any* LOCC protocol.

Various attempts have been made to minimize E. In [3], Eisert *et al.* discovered a protocol that implements any two-qubit *controlled*-unitary operation using LOCC assisted by a two-qubit maximally entangled state, or 1 *ebit* of entanglement. Hence, for two-qubit controlled-unitary operations, the minimum entanglement is upper bounded by 1 ebit. Since the maximum amount of entanglement created by performing a unitary operation, called its entangling power [4], cannot exceed its minimum entanglement cost, we can conclude that the minimum entanglement cost of a controlled-unitary operation is 1 ebit if its entangling power is also 1 ebit. A controlled-NOT operation and its local unitary equivalents are examples. However, the minimum entanglement cost for general controlled-unitary operations has been an open question for a decade.

In order to estimate the minimum entanglement cost, let us consider the case where the input state for the LOCC implementation of U is a pure product state. If the identity of the input is also provided at the beginning of the implementation (but only after the preparation of the resource state), then we can employ an input-dependent LOCC implementation protocol. In this case, LOCC implementability reduces to LOCC convertibility [5] between the two joint states of the input and resource system before and after performing U. If U is a two-qubit controlled-unitary operation denoted by U_u, it can generate states with a Schmidt number up to 2. For any given two pure entangled states with Schmidt number 2, one can be converted to the other by LOCC if and only if the former is more entangled than the latter. Hence, if the resource state has as much entanglement as the entangling power of U_u and Schmidt number 2, the LOCC implementation of U_u on a known pure product state is possible.

Because the entangling power of U_u is less than 1 ebit in general [4], this might make it natural to expect that U_u can be implemented using less than 1 ebit of entanglement resource with Schmidt number 2, even if the identity of the state remains unknown. Indeed, when the deterministicity condition has been relaxed, it is known that there is a situation where the average entanglement consumption can be reduced below 1 ebit in the asymptotic limit [6].

In this Letter, however, we prove that for determinis-

tic cases, LOCC implementation for any given two-qubit controlled-unitary operation on *unknown* inputs requires *at least* 1 ebit irrespective of its entangling power, when the resource is given by a bipartite entangled state with Schmidt number 2. Our result answers this long open question in entanglement theory.

The proof proceeds in the following four steps. First, we show that any LOCC implementation protocol must be such that the number of each party's local measurements, or *turns*, is greater than or equal to 3. Second, we present reductions of the descriptions of controlled-unitary operations and resource entanglement, using local unitary equivalence. Third, we show that any $(n > 3)$-turn LOCC implementation of a controlled-unitary operation can be transformed to an $(n - 1)$-turn protocol by investigating three cases that cover all possible LOCC implementation protocols for controlled-unitary operations. Finally, by induction, we see that an n-turn implementation protocol can be converted to a 3-turn one, for which it is proved that the amount of entanglement of the resource state must be 1 ebit.

We start by describing a LOCC implementation mathematically. $\mathcal{H}_{\text{in}}$ and $\mathcal{H}_{\text{r}}$ will be used to denote the Hilbert space of the input system and the resource system, respectively. We use $\{|0\rangle, |1\rangle\}$ as a basis for a qubit Hilbert space. To specify the Hilbert space where a given state belongs, we use the corresponding subscripts in both vector and operator notations, *e.g.*, $|0\rangle_X \in \mathcal{H}_X$ and $\rho_X \in \mathcal{S}(\mathcal{H}_X)$ for the Hilbert space $\mathcal{H}_X$. A LOCC implementation of a unitary operation U on $\mathcal{H}_{\text{in}}$ assisted by a given entangled state represented by ρ_{r} is a completely positive and trace-preserving (CPTP) map $\Gamma : \mathcal{S}(\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{r}}) \longrightarrow \mathcal{S}(\mathcal{H}_{\text{in}})$, such that it is implementable by LOCC and satisfies

$$\Gamma(\rho_{\text{in}} \otimes \rho_{\text{r}}) = U\rho_{\text{in}}U^\dagger \tag{1}$$

for all input states ρ_{in}. The state ρ_{r} is a resource state for such a LOCC implementation of U.

The input system consists of two parts, namely, Alice's input qubit and Bob's input qubit, whose corresponding Hilbert spaces are denoted by $\mathcal{H}_{A,\text{in}}$ and $\mathcal{H}_{B,\text{in}}$, respectively. The resource system also consists of a bipartite system shared between Alice and Bob, where the corresponding Hilbert spaces are denoted by $\mathcal{H}_{A,\text{r}}$ and $\mathcal{H}_{B,\text{r}}$. We call $\mathcal{H}_{A,\text{in}} \otimes \mathcal{H}_{A,\text{r}}$ *Alice's subsystem* and $\mathcal{H}_{B,\text{in}} \otimes \mathcal{H}_{B,\text{r}}$ *Bob's subsystem*, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are used to denote the Hilbert space corresponding to each party's subsystem. We will sometimes abbreviate $|k\rangle_{A,\text{in}} \otimes |l\rangle_{B,\text{in}}$ as $|kl\rangle_{\text{in}}$ and $|k\rangle_{A,\text{r}} \otimes |l\rangle_{B,\text{r}}$ as $|kl\rangle_{\text{r}}$.

At each turn in a general two-party LOCC protocol, either Alice or Bob performs any generalized measurement operation, which is described by two sets of measurement operators $\{M^{(r)}\}_r$ for Alice and $\{K^{(r)}\}_r$ for Bob, where r denotes a measurement outcome on each subsystem, and then classically communicates r to the other party. Note that unitary operations on each subsystem are included

as a special case where r has only one value. Since the only constraint on the set of measurement operators is the completeness relation, and operations at each turn can depend arbitrarily on the previous turns, the set of possible generalized measurement operations in LOCC is very large.

In order to manage this set, we focus on the accumulated effect that is brought on by successive operations in a given LOCC protocol. Let r_k denote the measurement outcome of the k-th turn, and $\vec{R}_k = (r_1, r_2, \ldots, r_k)$ denote the sequence of measurement outcomes of the first k turns. The kth generalized measurement operation is a function of $\vec{R}_{k-1}$. With a slight abuse of notation, we set $\vec{R}_k = (\vec{R}_{k-1}, r_k) = (\vec{R}_{k-2}, r_{k-1}, r_k) = \ldots$ and so on.

We use $M^{(r_k|\vec{R}_{k-1})}$ and $K^{(r_k|\vec{R}_{k-1})}$ to denote Alice's and Bob's measurement operators at the kth turn, respectively. To make the definition consistent, if the k-th turn is not Alice's turn to perform an operation, we set $M^{(r_k|\vec{R}_{k-1})} = \mathbb{I}_A$, where $\mathbb{I}_A$ is the identity operator on $\mathcal{H}_A$. Bob's measurement operators are defined similarly.

We define *accumulated operators* $A^{\vec{R}_k}$ and $B^{\vec{R}_k}$ that represent the accumulated effect of the measurement operators after k turns on Alice's and Bob's qubits, respectively, by $A^{\vec{R}_k} = M^{(r_k|\vec{R}_{k-1})}M^{(r_{k-1}|\vec{R}_{k-2})} \cdots M^{(r_1|\vec{R}_0)}$ and $B^{\vec{R}_k} = K^{(r_k|\vec{R}_{k-1})}K^{(r_{k-1}|\vec{R}_{k-2})} \cdots K^{(r_1|\vec{R}_0)}$, where $M^{(r_1|\vec{R}_0)} = M^{(r_1)}$ and $K^{(r_1|\vec{R}_0)} = K^{(r_1)}$. The accumulated operators naturally form a tree graph where each set of outcomes $\vec{R}_k$ labels a *branch* of length k.

The lengths of the branches in a LOCC protocol are not necessarily the same, but Alice and Bob can repeatedly perform identity operations to fill the shorter ones so that all branches have the same length n. Hence, we only need to consider protocols such that the target operation U is implemented after n turns. With this reduction and rewriting the CPTP map using accumulated operators $A^{\vec{R}_n}$ and $B^{\vec{R}_n}$, Eq. (1) now reads $\sum_{\vec{R}_n} (A^{\vec{R}_n} \otimes B^{\vec{R}_n})(\rho_{\text{in}} \otimes \rho_{\text{r}})(A^{\vec{R}_n} \otimes B^{\vec{R}_n})^\dagger = U\rho_{\text{in}}U^\dagger$.

Because U is a unitary operation, $U\rho_{\text{in}}U^\dagger$ is a pure state when ρ_{in} is pure. Thus, for each term in the summation, deterministicity requires a positive coefficient $p^{\vec{R}_n}$ exist such that

$$(A^{\vec{R}_n} \otimes B^{\vec{R}_n})(\rho_{\text{in}} \otimes \rho_{\text{r}})(A^{\vec{R}_n} \otimes B^{\vec{R}_n})^\dagger = p^{\vec{R}_n} U\rho_{\text{in}}U^\dagger. \tag{2}$$

From this equation, we can see that a mixed state $\rho_{\text{r}} = \sum_k p_k |\psi_k\rangle\langle\psi_k|$ is a resource state if and only if each of $|\psi_k\rangle\langle\psi_k|$ can be used as a resource. From here on, we only consider pure states for the entanglement resource.

As the first step of our proof, we show that the number of turns, n, must be greater than or equal to 3. It is shown in [7] that if a global unitary operation U is implementable by a LOCC protocol between Alice and Bob, the same protocol can be used for sending nonzero classical information from Alice to Bob or vice versa by choosing an appropriate input state for each party. There-

fore, if LOCC implementation of U with $n = 2$ turns is possible, a one-way LOCC protocol from Alice to Bob should be possible to send classical information from Bob to Alice. However, such a one-way LOCC protocol cannot change Alice's reduced density matrix depending on Bob's input state, hence, classical communication from Bob to Alice is impossible. Thus, taking the contrapositive, LOCC implementation of U with $n = 2$ turns is impossible. Impossibility with $n = 1$ protocols is trivial.

The argument so far holds for LOCC implementation of arbitrary (nontrivial) two-qubit unitary operations. We proceed to the second step of our proof by specifying them to be controlled-unitary operations. A general form is then given by $U_u = v_1 \otimes v_2 \cdot (|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes u) \cdot w_1 \otimes w_2$, where v_1, v_2, u, w_1, w_2 are single-qubit local unitary operations. U_u can be further locally transformed to

$$U_\theta = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + e^{i\theta}|11\rangle\langle 11| \quad (3)$$

where θ is a nonlocal parameter, by performing appropriate local unitary operations that depend only upon U_u. The local unitary operations taking U_u to U_θ are known to both Alice and Bob, so without loss of generality we only need to consider protocols implementing the single-parameter family U_θ.

In this step, we also specify our resource to be a bipartite entangled pure state with Schmidt number (the number of nonzero coefficients in its Schmidt decomposition) 2. Since any such state can be transformed into a two-qubit entangled state by local unitary operations, we can reduce the form of this resource state to $|r\rangle_r = (X_{A,r} \otimes \mathbb{I}_{B,r})|\Phi^+\rangle_r$, where $X \equiv \sqrt{\mu}|0\rangle\langle 0| + \sqrt{(1-\mu)}|1\rangle\langle 1|$ is a Choi matrix [8] and $|\Phi^+\rangle_r \equiv |00\rangle_r + |11\rangle_r$, by taking an appropriate choice of basis. With these notations, Eq. (2) now reads

$$(A^{\vec{R}_n} \otimes B^{\vec{R}_n})(|ij\rangle_{\text{in}} \otimes |r\rangle_r) = c^{\vec{R}_n}(U_\theta|ij\rangle_{\text{in}}) \quad (4)$$

for all $|ij\rangle_{\text{in}}$ and some input-independent $c^{\vec{R}_n} \in \mathbb{C}$ such that $|c^{\vec{R}_n}|^2 = p^{\vec{R}_n}$ for all $\vec{R}_n$.

We now proceed to the third and most demanding step of our proof. As $A^{\vec{R}_n}$ and $B^{\vec{R}_n}$ are operators taking a four-dimensional Hilbert space to a two-dimensional Hilbert space, by introducing unnormalized states $|a_{ki}^{\vec{R}_n}\rangle_{A,r}$ and $|b_{lj}^{\vec{R}_n}\rangle_{B,r}$, we have

$$A^{\vec{R}_n} = \sum_{k,i=0,1} |k\rangle_{A,\text{in}}\langle i| \otimes \langle a_{ki}^{\vec{R}_n}|_{A,r}, \quad (5)$$

$$B^{\vec{R}_n} = \sum_{l,j=0,1} |l\rangle_{B,\text{in}}\langle j| \otimes \langle b_{lj}^{\vec{R}_n}|_{B,r}. \quad (6)$$

For clarity, the subscripts of states will be dropped from here on. Equation (4) now implies the following conditions,

$$\langle a_{ki}^{\vec{R}_n}|X|b_{lj}^{\vec{R}_n*}\rangle = \begin{cases} c^{\vec{R}_n}\langle ij|U_\theta|ij\rangle & k=i \text{ and } l=j \\ 0 & \text{otherwise,} \end{cases} \quad (7)$$

where we have used $|b_{lj}^{\vec{R}_n*}\rangle$ to denote the complex conjugate of $|b_{lj}^{\vec{R}_n}\rangle$ in the $\{|0\rangle, |1\rangle\}$ basis. The vectors $\langle a_{00}^{\vec{R}_n}|$ and $\langle a_{11}^{\vec{R}_n}|$ must be linearly independent because $e^{i\theta} \neq 1$, and for the same reason so must $\langle b_{00}^{\vec{R}_n}|$ and $\langle b_{11}^{\vec{R}_n}|$ be. It is easy to show that $\langle a_{ki}^{\vec{R}_n}|$ and $\langle b_{lj}^{\vec{R}_n}|$ must be zero-vectors if $k \neq i$ and $l \neq j$, respectively. Therefore, $A^{\vec{R}_n}$ and $B^{\vec{R}_n}$ have the following forms

$$A^{\vec{R}_n} = |0\rangle\langle 0| \otimes \langle a_{00}^{\vec{R}_n}| + |1\rangle\langle 1| \otimes \langle a_{11}^{\vec{R}_n}|, \quad (8)$$

$$B^{\vec{R}_n} = |0\rangle\langle 0| \otimes \langle b_{00}^{\vec{R}_n}| + |1\rangle\langle 1| \otimes \langle b_{11}^{\vec{R}_n}|. \quad (9)$$

Without loss of generality we now consider the case where Bob performs the final (n-th) turn in an implementation protocol. As defined above, the accumulated operators for the previous three turns then satisfy the following relations:

$$A^{\vec{R}_{n-1}} = A^{\vec{R}_n} = A^{(\vec{R}_{n-1}, r_n)}, \quad (10)$$

$$A^{\vec{R}_{n-2}\dagger}A^{\vec{R}_{n-2}} = \sum_{r_{n-1}} A^{(\vec{R}_{n-2}, r_{n-1})\dagger}A^{(\vec{R}_{n-2}, r_{n-1})}, \quad (11)$$

$$A^{\vec{R}_{n-3}} = A^{\vec{R}_{n-2}} = A^{(\vec{R}_{n-3}, r_{n-2})}, \quad (12)$$

and

$$B^{\vec{R}_{n-1}\dagger}B^{\vec{R}_{n-1}} = \sum_{r_n} B^{(\vec{R}_{n-1}, r_n)\dagger}B^{(\vec{R}_{n-1}, r_n)}, \quad (13)$$

$$B^{\vec{R}_{n-2}} = B^{\vec{R}_{n-1}} = B^{(\vec{R}_{n-2}, r_{n-1})}, \quad (14)$$

$$B^{\vec{R}_{n-3}\dagger}B^{\vec{R}_{n-3}} = \sum_{r_{n-2}} B^{(\vec{R}_{n-3}, r_{n-2})\dagger}B^{(\vec{R}_{n-3}, r_{n-2})}. \quad (15)$$

We show that any ($n \geq 3$)-turn LOCC protocol implementing U_θ can be transformed into a ($n - 1$)-turn LOCC protocol by investigating three types of transformations conditioned on the accumulated operators that arise at the ($n-3$)-th turn, $A^{\vec{R}_{n-3}}$ and $B^{\vec{R}_{n-3}}$. A rigorous proof for all three cases requires intensive analysis of the relations that hold for the accumulated operators, and is given in the supplementary material [9]. In what follows, we concentrate on that which is important for understanding the three transformations.

Defining the block elements $A_{kk}^{\vec{R}_{n-3}}$ and $B_{ll}^{\vec{R}_{n-3}}$ of the accumulated operators $A^{\vec{R}_{n-3}}$ and $B^{\vec{R}_{n-3}}$ by

$$A_{kk}^{\vec{R}_{n-3}} = \sqrt{\sum_{r_{n-1}} |a_{kk}^{\vec{R}_n}\rangle\langle a_{kk}^{\vec{R}_n}|}, \quad (16)$$

$$B_{ll}^{\vec{R}_{n-3}} = \sqrt{\sum_{r_{n-2}, r_n} |b_{ll}^{\vec{R}_n}\rangle\langle b_{ll}^{\vec{R}_n}|}, \quad (17)$$

and using Eqs. (8) to (15), we obtain the following relations

$$A^{\vec{R}_{n-3}\dagger}A^{\vec{R}_{n-3}} = \sum_{k=0,1} |k\rangle\langle k| \otimes (A_{kk}^{\vec{R}_{n-3}})^2, \quad (18)$$

$$B^{\vec{R}_{n-3}\dagger}B^{\vec{R}_{n-3}} = \sum_{l=0,1} |l\rangle\langle l| \otimes (B_{ll}^{\vec{R}_{n-3}})^2. \quad (19)$$

The ranks of $A_{kk}^{\vec{R}_{n-3}}$ and $B_{ll}^{\vec{R}_{n-3}}$ cannot be taken independently for successful LOCC implementable protocols. Indeed, we have the following lemma, whose proof is given in [9].

Lemma 1. *The ranks of $A_{00}^{\vec{R}_{n-3}}$ and $A_{11}^{\vec{R}_{n-3}}$ must be the same for any successful protocol. Additionally, if the rank of $A_{00}^{\vec{R}_{n-3}}$ is 2, the ranks of $B_{00}^{\vec{R}_{n-3}}$ and $B_{11}^{\vec{R}_{n-3}}$ must be the same.*

This implies that all successful protocols can be classified into the following three cases; (a) rank $A_{00}^{\vec{R}_{n-3}} = 1$ (b) rank $A_{00}^{\vec{R}_{n-3}} = 2$, rank $B_{00}^{\vec{R}_{n-3}} = 1$ (c) rank $A_{00}^{\vec{R}_{n-3}} = 2$, rank $B_{00}^{\vec{R}_{n-3}} = 2$.

For cases (a) and (b), we have [9],

Lemma 2. *If rank $A_{00}^{\vec{R}_{n-3}} = 1$, then $\{M^{(r_{n-1}|\vec{R}_{n-2})}\}_{r_{n-1}}$ is simulateable by a random unitary operation $\{p^{\vec{R}_{n-1}}, U^{\vec{R}_{n-1}}\}$. On the other hand, if rank $B_{00}^{\vec{R}_{n-3}} = 1$, then $\{K^{(r_{n-2}|\vec{R}_{n-3})}\}_{r_{n-2}}$ can be simulated by a random unitary operation $\{q^{\vec{R}_{n-2}}, V^{\vec{R}_{n-2}}\}$.*

When the operation at a given turn is a random unitary operation, the "outcome" of the operation r_{n-1} for case (a) [or r_{n-2} for case (b)] can be *chosen* by Bob for case (a) [Alice for case (b)] and can be communicated with the measurement outcome r_{n-2} (or r_{n-3}). Then the communication of r_{n-1} from Alice to Bob (or r_{n-2} from Bob to Alice) is no longer necessary. Therefore, the number of turns can be decreased from n to $n-1$.

For case (c), we have [9, 10],

Lemma 3. *If rank $A_{00}^{\vec{R}_{n-3}} = $ rank $B_{00}^{\vec{R}_{n-3}} = 2$, then it is possible to replace $\{K^{(r_{n-2}|\vec{R}_{n-3})}\}_{r_{n-2}}$, $\{M^{(r_{n-1}|\vec{R}_{n-2})}\}_{r_{n-1}}$, and $\{K^{(r_n|\vec{R}_{n-1})}\}_{r_n}$ with $\{M'^{(r_{n-2}|\vec{R}_{n-3})}\}_{r_{n-2}}$, $\{K'^{(r_{n-1}|\vec{R}_{n-2})}\}_{r_{n-1}}$, and $\{M'^{(r_n|\vec{R}_{n-1})}\}_{r_n}$, without changing $A^{\vec{R}_m}$ and $B^{\vec{R}_m}$ for $m \leq n-3$.*

After this replacement, notice that the $(n-3)$th turn and $(n-2)$th turn are both performed by Alice. These turns can be combined into a single operation, reducing the total number of turns from n to $n-1$.

Hence, for all three types of successful implementation protocols with $n \geq 3$ the total number of turns can be decreased by one. By induction, all implementation protocols can be transformed to one with three turns.

In the final step of our proof, we show the necessity of a 1-ebit resource. The following lemma is proved in [9].

Lemma 4. *Suppose $n \geq 3$. If rank $A_{00}^{\vec{R}_{n-3}} = 2$ and $A_{11}^{\vec{R}_{n-3}}(A_{00}^{\vec{R}_{n-3}})^{-1}$ is a unitary operation, then*

$$\sum_l A_{00}^{\vec{R}_{n-3}} X^t B_{ll}^{\vec{R}_{n-3}} \cdot (c.c.) \propto \mathbb{I}. \tag{20}$$

For a 3-turn LOCC protocol, $A^{\vec{R}_{n-3}}$ and $B^{\vec{R}_{n-3}}$ are the identity operator by definition. Clearly, Lemma 4 can be applied and Eq. (20) now reads, $\sum_l X^2 \propto I$. Because X is a positive matrix, we see that $X \propto I$. By the definition of X, we have that the resource state should be given by $|r\rangle = |\Phi^+\rangle/\sqrt{2}$, which has 1 ebit of entanglement.

In this letter, we analyzed deterministic entanglement-assisted LOCC implementation of two-qubit controlled-unitary operations and showed that any given two-qubit controlled-unitary operation can be implemented by a three-turn protocol, which requires at least 1 ebit of entanglement when the resource is given by a bipartite entangled state with Schmidt number 2. Our result implies that such a protocol necessarily consumes more entanglement than it can create, raising interesting questions about connections to irreversibility. This gap between the minimum entanglement cost and entangling power arises due to the requirement of implementation without knowing the inputs, since entanglement cost can be reduced by implementing an input-dependent protocol.

Our result also indicates that, since it is possible to realize a controlled-unitary operation by composing several controlled-unitary operations with less entangling power, such a decomposition consumes much more entanglement than when the target controlled-unitary operation is directly implemented. Finally, our proofs are constructive, in that we explicitly give the new protocol that achieves the implementation in fewer steps.

[1] J.I. Cirac, A.K. Ekert, S.F. Huelga and C. Machiavello, *Phys. Rev. A* **59**, 4249 (1999); H. Buhrman and H. Röhrig, in *Lecture Notes in Computer Science* **2747** (Springer 2003), 1.

[2] M.J. Donald, M. Horodecki, and O. Rudolph, *J. Math. Phys.* **43**, 4252 (2002).

[3] J. Eisert, K. Jacobs, P. Papadopoulos and M.B. Plenio. *Phys. Rev. A.* **62** 052317, 2000.

[4] B. Kraus and J. I. Cirac, *Phys. Rev. A* **63**, 062309 (2001)

[5] M.A. Nielsen, *Phys. Rev. Lett.* **83**, 436 (1999).

[6] J.I. Cirac, W. Dür, B. Kraus and M. Lewenstein, *Phys. Rev. Lett.* **86** 544, 2001.

[7] C. H. Bennett, A. W. Harrow, D. W. Leung and J. A. Smolin, *IEEE Trans. Inf. Theory* **49**, 1895 (2003).

[8] M. Choi, *Lin. Alg. Appl.* **10**, 285 (1975).

[9] See Appendix.

[10] E. Andersson and D.K.L. Oi, *Phys. Rev. A* **77**, 052104 (2008).

[11] D. Stahlke and R. B. Griffiths, *Phys. Rev. A* **84**, 032316 (2011).

Proof of Lemma 1

In this section, we provide a proof of Lemma 1, which is divided into two subsections, the first for the A operators and the second for the B operators. The calculations presented here are also used in the subsequent proofs.

The proof for $\operatorname{rank} A_{00}^{\vec{R}_{n-3}} = \operatorname{rank} A_{11}^{\vec{R}_{n-3}}$

In this section, we show the ranks of the block elements of accumulated operators $A_{kk}^{\vec{R}_{n-3}}$ for $k = 0$ and $k = 1$ should be same for successful LOCC implementation of controlled-unitary operations.

For any given $\vec{R}_n$, $c^{\vec{R}_n}$, and a full rank X, there always exists a unique pair of linearly independent vectors $\{\langle b_{00}^{\vec{R}_n}|, \langle b_{11}^{\vec{R}_n}|\}$ corresponding to the linearly independent vectors $\{\langle a_{00}^{\vec{R}_n}|, \langle a_{11}^{\vec{R}_n}|\}$. To see this, first recall that $\langle a_{00}^{\vec{R}_n}|$ and $\langle a_{11}^{\vec{R}_n}|$ are linearly independent, therefore, (due to their Hilbert spaces being isomorphic), it is possible to decompose $|b_{00}^{\vec{R}_n*}\rangle$ and $|b_{11}^{\vec{R}_n*}\rangle$ as

$$|b_{00}^{\vec{R}_n*}\rangle = x^{\vec{R}_n}|a_{00}^{\vec{R}_n}\rangle + y^{\vec{R}_n}|a_{11}^{\vec{R}_n}\rangle$$

and

$$|b_{11}^{\vec{R}_n*}\rangle = \xi^{\vec{R}_n}|a_{00}^{\vec{R}_n}\rangle + \eta^{\vec{R}_n}|a_{11}^{\vec{R}_n}\rangle.$$

Substituting these equations into Eq. (7), we obtain

$$x^{\vec{R}_n}\langle a_{00}^{\vec{R}_n}|X|a_{00}^{\vec{R}_n}\rangle + y^{\vec{R}_n}\langle a_{00}^{\vec{R}_n}|X|a_{11}^{\vec{R}_n}\rangle = c^{\vec{R}_n},$$
$$x^{\vec{R}_n}\langle a_{11}^{\vec{R}_n}|X|a_{00}^{\vec{R}_n}\rangle + y^{\vec{R}_n}\langle a_{11}^{\vec{R}_n}|X|a_{11}^{\vec{R}_n}\rangle = c^{\vec{R}_n},$$
$$\xi^{\vec{R}_n}\langle a_{00}^{\vec{R}_n}|X|a_{00}^{\vec{R}_n}\rangle + \eta^{\vec{R}_n}\langle a_{00}^{\vec{R}_n}|X|a_{11}^{\vec{R}_n}\rangle = c^{\vec{R}_n},$$
$$\xi^{\vec{R}_n}\langle a_{11}^{\vec{R}_n}|X|a_{00}^{\vec{R}_n}\rangle + \eta^{\vec{R}_n}\langle a_{11}^{\vec{R}_n}|X|a_{11}^{\vec{R}_n}\rangle = c^{\vec{R}_n}e^{i\theta}.$$

Defining a matrix $L^{\vec{R}_n}$ by

$$L^{\vec{R}_n} = \begin{pmatrix} \langle a_{00}^{\vec{R}_n}|X|a_{00}^{\vec{R}_n}\rangle & \langle a_{00}^{\vec{R}_n}|X|a_{11}^{\vec{R}_n}\rangle \\ \langle a_{11}^{\vec{R}_n}|X|a_{00}^{\vec{R}_n}\rangle & \langle a_{11}^{\vec{R}_n}|X|a_{11}^{\vec{R}_n}\rangle \end{pmatrix},$$

the four equations above are equivalent to

$$L^{\vec{R}_n} \cdot \begin{pmatrix} x^{\vec{R}_n} \\ y^{\vec{R}_n} \end{pmatrix} = c^{\vec{R}_n} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \tag{21}$$

$$L^{\vec{R}_n} \cdot \begin{pmatrix} \xi^{\vec{R}_n} \\ \eta^{\vec{R}_n} \end{pmatrix} = c^{\vec{R}_n} \begin{pmatrix} 1 \\ e^{i\theta} \end{pmatrix}. \tag{22}$$

We denote the elements of $(L^{\vec{R}_n})^{-1}$ as

$$(L^{\vec{R}_n})^{-1} = \begin{pmatrix} (L^{\vec{R}_n})_{00}^{-1} & (L^{\vec{R}_n})_{01}^{-1} \\ (L^{\vec{R}_n})_{10}^{-1} & (L^{\vec{R}_n})_{11}^{-1} \end{pmatrix}.$$

With this notation, we have

$$x^{\vec{R}_n} = c^{\vec{R}_n}((L^{\vec{R}_n})_{00}^{-1} + (L^{\vec{R}_n})_{01}^{-1}),$$
$$y^{\vec{R}_n} = c^{\vec{R}_n}((L^{\vec{R}_n})_{10}^{-1} + (L^{\vec{R}_n})_{11}^{-1},)$$
$$\xi^{\vec{R}_n} = c^{\vec{R}_n}((L^{\vec{R}_n})_{00}^{-1} + e^{i\theta}(L^{\vec{R}_n})_{01}^{-1}),$$
$$\eta^{\vec{R}_n} = c^{\vec{R}_n}((L^{\vec{R}_n})_{10}^{-1} + e^{i\theta}(L^{\vec{R}_n})_{11}^{-1}).$$

Note that the right hand side is determined by $\{\langle a_{00}^{\vec{R}_n}|, \langle a_{11}^{\vec{R}_n}|, c^{\vec{R}_n}, X\}$, therefore $\langle b_{00}^{\vec{R}_n}|$ and $\langle b_{11}^{\vec{R}_n}|$ are unique functions of $\{\langle a_{00}^{\vec{R}_n}|, \langle a_{11}^{\vec{R}_n}|, c^{\vec{R}_n}, X\}$.

This uniqueness of $\langle b_{ll}^{\vec{R}_n}|$ to $\{\langle a_{kk}^{\vec{R}_n}|, c^{\vec{R}_n}, X\}$ implies that the dependence of $\langle b_{ll}^{\vec{R}_n}|$ of r_n is only through $c^{\vec{R}_n}$. To see this, for any given $\vec{R}_{n-1}$ and r_n, Eq. (10) implies that $A^{(\vec{R}_{n-1}, r_n)}$ does not have any r_n-dependence which means that $\langle a_{00}^{\vec{R}_n}|$ and $\langle a_{11}^{\vec{R}_n}|$ should also not have this r_n-dependence, $i.e.$,

$$\langle a_{00}^{(\vec{R}_{n-1}, r_n)}| = \langle a_{00}^{(\vec{R}_{n-1}, r'_n)}|, \tag{23}$$
$$\langle a_{11}^{(\vec{R}_{n-1}, r_n)}| = \langle a_{11}^{(\vec{R}_{n-1}, r'_n)}| \tag{24}$$

for any r_n and r'_n. We define $\langle a_{00}^{\vec{R}_{n-1}}|$ and $\langle a_{11}^{\vec{R}_{n-1}}|$ by

$$\langle a_{00}^{\vec{R}_{n-1}}| = \langle a_{00}^{(\vec{R}_{n-1}, 0)}|, \tag{25}$$
$$\langle a_{11}^{\vec{R}_{n-1}}| = \langle a_{11}^{(\vec{R}_{n-1}, 0)}| \tag{26}$$

Using this notation, we have, similar to Eq.(8),

$$A^{\vec{R}_{n-1}} = |0\rangle\langle 0| \otimes \langle a_{00}^{\vec{R}_{n-1}}| + |1\rangle\langle 1| \otimes \langle a_{11}^{\vec{R}_{n-1}}|. \tag{27}$$

It must be that $L^{\vec{R}_n}$, whose r_n-dependence is only through $\langle a_{00}^{\vec{R}_n}|$ and $\langle a_{11}^{\vec{R}_n}|$, is independent of r_n, from which we learn that

$$\langle b_{00}^{(\vec{R}_{n-1}, r_n)}| = \frac{c^{(\vec{R}_{n-1}, r_n)}}{c^{(\vec{R}_{n-1}, r'_n)}}\langle b_{00}^{(\vec{R}_{n-1}, r'_n)}|, \tag{28}$$

$$\langle b_{11}^{(\vec{R}_{n-1}, r_n)}| = \frac{c^{(\vec{R}_{n-1}, r_n)}}{c^{(\vec{R}_{n-1}, r'_n)}}\langle b_{11}^{(\vec{R}_{n-1}, r'_n)}|. \tag{29}$$

Therefore, for two different outcomes r_n and r'_n, $\langle b_{ll}^{(\vec{R}_{n-1}, r_n)}|$ and $\langle b_{ll}^{(\vec{R}_{n-1}, r'_n)}|$ are collinear.

Defining $\gamma^{\vec{R}_n}$ by

$$\gamma^{\vec{R}_n} = \frac{c^{(\vec{R}_{n-1}, r_n)}}{c^{(\vec{R}_{n-1}, 0)}}, \tag{30}$$

and using Eq. (13), we see that

$$B^{\vec{R}_{n-1}\dagger}B^{\vec{R}_{n-1}} = \sum_{r_n} B^{(\vec{R}_{n-1},r_n)\dagger}B^{(\vec{R}_{n-1},r_n)}$$

$$= \sum_{r_n} |0\rangle\langle 0| \otimes |\gamma^{(\vec{R}_{n-1},r_n)}|^2|b_{00}^{(\vec{R}_{n-1},0)}\rangle\langle b_{00}^{(\vec{R}_{n-1},0)}|$$

$$+ |1\rangle\langle 1| \otimes |\gamma^{(\vec{R}_{n-1},r_n)}|^2|b_{11}^{(\vec{R}_{n-1},0)}\rangle\langle b_{11}^{(\vec{R}_{n-1},0)}|$$

$$= |0\rangle\langle 0| \otimes (\sum_{r_n}|\gamma^{(\vec{R}_{n-1},r_n)}|^2)|b_{00}^{(\vec{R}_{n-1},0)}\rangle\langle b_{00}^{(\vec{R}_{n-1},0)}|$$

$$+ |1\rangle\langle 1| \otimes (\sum_{r_n}|\gamma^{(\vec{R}_{n-1},r_n)}|^2)|b_{11}^{(\vec{R}_{n-1},0)}\rangle\langle b_{11}^{(\vec{R}_{n-1},0)}|.$$

Here we prove a claim on the relationship between the square moduli of two $n \times m$ complex matrices.

Claim 1. *Let $M_{m,n}$ denote the set of $m \times n$ complex matrices. If two linear operators $T \in M_{m,n}$ and $T' \in M_{m',n}$ satisfy*

$$T^{\dagger}T = T'^{\dagger}T', \tag{31}$$

then there exists an isometry U such that

$$T' = UT.$$

Proof. We define

$$H = T^{\dagger}T. \tag{32}$$

T has a polar decomposition

$$T = U\sqrt{H}, \tag{33}$$

where U is an isometry satisfying

$$U^{\dagger}U = \mathbb{I}_{n\times n}.$$

Here, $\mathbb{I}_{n\times n}$ denotes the $n \times n$ identity operator. Eqs. (31) and (32) imply that there exists an isometry U' such that

$$T' = U'\sqrt{H},$$

where U' is an isometry satisfying

$$U'^{\dagger}U' = \mathbb{I}_{n\times n}.$$

We define a new isometry

$$V = U'U^{\dagger}.$$

We see that

$$T' = VT$$

because

$$VT = U'U^{\dagger}T = U'U^{\dagger}U\sqrt{H}$$
$$= U' \cdot \mathbb{I}_{n\times n} \cdot \sqrt{H} = U'\sqrt{H} = T'.$$

$\square$

Using Claim 1 and setting $g^{\vec{R}_{n-1}}$ to be

$$g^{\vec{R}_{n-1}} = \sqrt{\sum_{r_n}|\gamma^{(\vec{R}_{n-1},r_n)}|^2}, \tag{34}$$

we see that there exists an isometry $U_B^{\vec{R}_{n-1}}$ such that

$$B^{\vec{R}_{n-1}} = U_B^{\vec{R}_{n-1}} \cdot (|0\rangle\langle 0| \otimes g^{\vec{R}_{n-1}}\langle b_{00}^{(\vec{R}_{n-1},0)}|$$
$$+ |1\rangle\langle 1| \otimes g^{\vec{R}_{n-1}}\langle b_{11}^{(\vec{R}_{n-1},0)}|). \tag{35}$$

By introducing the following notation

$$\langle b_{00}^{\vec{R}_{n-1}}| = g^{\vec{R}_{n-1}}\langle b_{00}^{(\vec{R}_{n-1},0)}|, \tag{36}$$

$$\langle b_{11}^{\vec{R}_{n-1}}| = g^{\vec{R}_{n-1}}\langle b_{11}^{(\vec{R}_{n-1},0)}|, \tag{37}$$

$B^{\vec{R}_{n-1}}$ is given by

$$B^{\vec{R}_{n-1}} = U_B^{\vec{R}_{n-1}} \cdot (|0\rangle\langle 0|\otimes\langle b_{00}^{\vec{R}_{n-1}}|+|1\rangle\langle 1|\otimes\langle b_{11}^{\vec{R}_{n-1}}|). \tag{38}$$

We also define

$$\langle b_{00}^{\vec{R}_{n-2}}| = \langle b_{00}^{(\vec{R}_{n-2},0)}|, \tag{39}$$

$$\langle b_{11}^{\vec{R}_{n-2}}| = \langle b_{11}^{(\vec{R}_{n-2},0)}|. \tag{40}$$

Eq. (14) implies that

$$B^{(\vec{R}_{n-2},0)\dagger}B^{(\vec{R}_{n-2},0)} = B^{(\vec{R}_{n-2},r_{n-1})\dagger}B^{(\vec{R}_{n-2},r_{n-1})}. \tag{41}$$

Using Eq. (38), Eq. (41) is equivalent to

$$|b_{00}^{\vec{R}_{n-2}}\rangle\langle b_{00}^{\vec{R}_{n-2}}| = |b_{00}^{(\vec{R}_{n-2},r_{n-1})}\rangle\langle b_{00}^{(\vec{R}_{n-2},r_{n-1})}|, \tag{42}$$

$$|b_{11}^{\vec{R}_{n-2}}\rangle\langle b_{11}^{\vec{R}_{n-2}}| = |b_{11}^{(\vec{R}_{n-2},r_{n-1})}\rangle\langle b_{11}^{(\vec{R}_{n-2},r_{n-1})}|. \tag{43}$$

For Eqs. (42) and (43) to hold, there must be phase factors $\exp[i\varphi_0^{(\vec{R}_{n-2},r_{n-1})}]$ and $\exp[i\varphi_1^{(\vec{R}_{n-2},r_{n-1})}]$ such that

$$\langle b_{00}^{\vec{R}_{n-2}}| = \exp[i\varphi_0^{(\vec{R}_{n-2},r_{n-1})}]\langle b_{00}^{(\vec{R}_{n-2},r_{n-1})}|, \tag{44}$$

$$\langle b_{11}^{\vec{R}_{n-2}}| = \exp[i\varphi_1^{(\vec{R}_{n-2},r_{n-1})}]\langle b_{11}^{(\vec{R}_{n-2},r_{n-1})}|. \tag{45}$$

On the other hand, the left hand side of Eq. (7) can be re-expressed as follows

$$\langle a_{kk}^{\vec{R}_n}|X|b_{ll}^{\vec{R}_n*}\rangle = \gamma^{\vec{R}_n}\langle a_{kk}^{\vec{R}_{n-1}}|X|b_{ll}^{(\vec{R}_{n-1},0)*}\rangle$$

$$= \frac{\gamma^{\vec{R}_n}}{g^{\vec{R}_{n-1}}}\langle a_{kk}^{\vec{R}_{n-1}}|X|b_{ll}^{\vec{R}_{n-1}*}\rangle$$

$$= \frac{\gamma^{\vec{R}_n}}{g^{\vec{R}_{n-1}}} \cdot e^{i\varphi_l^{(\vec{R}_{n-2},r_{n-1})}}\langle a_{kk}^{\vec{R}_{n-1}}|X|b_{ll}^{\vec{R}_{n-2}*}\rangle.$$

By defining

$$\kappa_l^{\vec{R}_n} = \frac{g^{\vec{R}_{n-1}}e^{-i\varphi_l^{\vec{R}_{n-1}}}c^{\vec{R}_n}}{\gamma^{\vec{R}_n}}$$

and

$$\mathcal{E}_{kl} = \langle kl|U_\theta|kl\rangle,$$

Eq. (7) is equivalent to

$$\langle a_{kk}^{\vec{R}_{n-1}}|X|b_{ll}^{\vec{R}_{n-2}*}\rangle = \kappa_l^{\vec{R}_n}\mathcal{E}_{kl}. \qquad (46)$$

Eq. (46) indicates that

$$\kappa_l^{(\vec{R}_{n-1},r_n)} = \kappa_l^{(\vec{R}_{n-1},r_n')}$$

for any r_n and r_n'. We define

$$\kappa_l^{\vec{R}_{n-1}} = \kappa_l^{(\vec{R}_{n-1},0)}.$$

By Eq. (11), we see that

$$A^{\vec{R}_{n-2}\dagger}A^{\vec{R}_{n-2}} = \sum_{r_{n-1}} |0\rangle\langle 0|\otimes|a_{00}^{(\vec{R}_{n-2},r_{n-1})}\rangle\langle a_{00}^{(\vec{R}_{n-2},r_{n-1})}|$$
$$+ |1\rangle\langle 1|\otimes|a_{11}^{(\vec{R}_{n-2},r_{n-1})}\rangle\langle a_{11}^{(\vec{R}_{n-2},r_{n-1})}|. \qquad (47)$$

Notice that

$$\sum_{r_{n-1}} |a_{00}^{(\vec{R}_{n-2},r_{n-1})}\rangle\langle a_{00}^{(\vec{R}_{n-2},r_{n-1})}| \qquad (48)$$

and

$$\sum_{r_{n-1}} |a_{11}^{(\vec{R}_{n-2},r_{n-1})}\rangle\langle a_{11}^{(\vec{R}_{n-2},r_{n-1})}|$$

are positive semidefinite operators. We may therefore define 2×2 matrices $A_{00}^{\vec{R}_{n-2}}$ and $A_{11}^{\vec{R}_{n-2}}$ by

$$A_{00}^{\vec{R}_{n-2}} = \sqrt{\sum_{r_{n-1}} |a_{00}^{(\vec{R}_{n-2},r_{n-1})}\rangle\langle a_{00}^{(\vec{R}_{n-2},r_{n-1})}|}, \qquad (49)$$

$$A_{11}^{\vec{R}_{n-2}} = \sqrt{\sum_{r_{n-1}} |a_{11}^{(\vec{R}_{n-2},r_{n-1})}\rangle\langle a_{11}^{(\vec{R}_{n-2},r_{n-1})}|}, \qquad (50)$$

analogous to Eq.(16). Using Eq. (46) and from the definition of $A_{kk}^{\vec{R}_{n-1}}$, we see that

$$\langle b_{00}^{\vec{R}_{n-2}*}|X(A_{00}^{\vec{R}_{n-2}})^2 X|b_{00}^{\vec{R}_{n-2}*}\rangle$$
$$= \sum_{r_{n-1}} |\kappa_0^{(\vec{R}_{n-2},r_{n-1})}|^2$$
$$= \langle b_{00}^{\vec{R}_{n-2}*}|X(A_{11}^{\vec{R}_{n-2}})^2 X|b_{00}^{\vec{R}_{n-2}*}\rangle \qquad (51)$$

$$\langle b_{11}^{\vec{R}_{n-2}*}|X(A_{00}^{\vec{R}_{n-2}})^2 X|b_{11}^{\vec{R}_{n-2}*}\rangle$$
$$= \sum_{r_{n-1}} |\kappa_1^{(\vec{R}_{n-2},r_{n-1})}|^2$$
$$= \langle b_{11}^{\vec{R}_{n-2}*}|X(A_{11}^{\vec{R}_{n-2}})^2 X|b_{11}^{\vec{R}_{n-2}*}\rangle \qquad (52)$$

and

$$\langle b_{00}^{\vec{R}_{n-2}*}|X(A_{00}^{\vec{R}_{n-2}})^2 X|b_{11}^{\vec{R}_{n-2}*}\rangle$$
$$= \sum_{r_{n-1}} (\kappa_0^{(\vec{R}_{n-2},r_{n-1})})^* \kappa_1^{(\vec{R}_{n-2},r_{n-1})}$$
$$= e^{-i\theta}\langle b_{00}^{\vec{R}_{n-2}*}|X(A_{11}^{\vec{R}_{n-2}})^2 X|b_{11}^{\vec{R}_{n-2}*}\rangle. \qquad (53)$$

In the definition of κ we see that the l dependence occurs only in a phase, and in particular

$$|\kappa_0^{\vec{R}_n}| = \left|\left(\frac{g^{\vec{R}_{n-1}}}{\gamma^{\vec{R}_n}}\right)^2 c^{\vec{R}_n}\right| = |\kappa_1^{\vec{R}_n}|,$$

therefore Eqs. (51) and (52) imply

$$\langle b_{00}^{\vec{R}_{n-2}*}|X(A_{00}^{\vec{R}_{n-2}})^2 X|b_{00}^{\vec{R}_{n-2}*}\rangle,$$
$$= \langle b_{11}^{\vec{R}_{n-2}*}|X(A_{00}^{\vec{R}_{n-2}})^2 X|b_{11}^{\vec{R}_{n-2}*}\rangle. \qquad (54)$$

For two vectors

$$A_{00}^{\vec{R}_{n-2}} X|b_{00}^{\vec{R}_{n-2}*}\rangle$$

and

$$A_{00}^{\vec{R}_{n-2}} X|b_{11}^{\vec{R}_{n-2}*}\rangle,$$

the Cauchy-Schwarz inequality requires that

$$\langle b_{00}^{\vec{R}_{n-2}*}|X(A_{00}^{\vec{R}_{n-2}})^2 X|b_{00}^{\vec{R}_{n-2}*}\rangle\times$$
$$\langle b_{11}^{\vec{R}_{n-2}*}|X(A_{00}^{\vec{R}_{n-2}})^2 X|b_{11}^{\vec{R}_{n-2}*}\rangle$$
$$- |\langle b_{00}^{\vec{R}_{n-2}*}|X(A_{00}^{\vec{R}_{n-2}})^2 X|b_{11}^{\vec{R}_{n-2}*}\rangle|^2 \geq 0. \qquad (55)$$

By Eqs. (51), (52), and (53), we also have that

$$\langle b_{00}^{\vec{R}_{n-2}*}|X(A_{11}^{\vec{R}_{n-2}})^2 X|b_{00}^{\vec{R}_{n-2}*}\rangle\times$$
$$\langle b_{11}^{\vec{R}_{n-2}*}|X(A_{11}^{\vec{R}_{n-2}})^2 X|b_{11}^{\vec{R}_{n-2}*}\rangle$$
$$- |\langle b_{00}^{\vec{R}_{n-2}*}|X(A_{11}^{\vec{R}_{n-2}})^2 X|b_{11}^{\vec{R}_{n-2}*}\rangle|^2 \geq 0. \qquad (56)$$

Notice that the equality condition of Eq. (55) holds if and only if the equality condition of Eq. (56) holds. From this, we conclude that $A_{00}^{\vec{R}_{n-2}} X|b_{00}^{\vec{R}_{n-2}*}\rangle$ and $A_{00}^{\vec{R}_{n-2}} X|b_{11}^{\vec{R}_{n-2}*}\rangle$ are linearly independent if and only if $A_{11}^{\vec{R}_{n-2}} X|b_{00}^{\vec{R}_{n-2}*}\rangle$ and $A_{11}^{\vec{R}_{n-2}} X|b_{11}^{\vec{R}_{n-2}*}\rangle$ are linearly independent.

Recall that X is full rank and observe that $|b_{00}^{\vec{R}_{n-2}*}\rangle$ and $|b_{11}^{\vec{R}_{n-2}*}\rangle$ are linearly independent, which can be seen by invoking Eqs. (39) and (40) to derive

$$|b_{00}^{\vec{R}_{n-2}*}\rangle \propto |b_{00}^{(\vec{R}_{n-2},0)*}\rangle \propto |b_{00}^{(\vec{R}_{n-2},0,0)*}\rangle$$
$$|b_{11}^{\vec{R}_{n-2}*}\rangle \propto |b_{11}^{(\vec{R}_{n-2},0)*}\rangle \propto |b_{11}^{(\vec{R}_{n-2},0,0)*}\rangle.$$

Now, if $A_{00}^{\vec{R}_{n-2}}$ is rank 1, then $A_{00}^{\vec{R}_{n-2}} X |b_{00}^{\vec{R}_{n-2}*}\rangle$ and $A_{00}^{\vec{R}_{n-2}} X |b_{11}^{\vec{R}_{n-2}*}\rangle$ are collinear, which means that so are $A_{11}^{\vec{R}_{n-2}} X |b_{00}^{\vec{R}_{n-2}*}\rangle$ and $A_{11}^{\vec{R}_{n-2}} X |b_{11}^{\vec{R}_{n-2}*}\rangle$. Therefore, $A_{11}^{\vec{R}_{n-2}}$ must also be rank 1. Switching the roles of $A_{00}^{\vec{R}_{n-2}}$ and $A_{11}^{\vec{R}_{n-2}}$, we see that $A_{11}^{\vec{R}_{n-2}}$ is rank 1 if and only if $A_{00}^{\vec{R}_{n-2}}$ is rank 1. Thus we arrive at the following relation

$$\text{rank } A_{00}^{\vec{R}_{n-2}} = \text{rank } A_{11}^{\vec{R}_{n-2}}, \tag{57}$$

and thus by Eq. (12) we have

$$\text{rank } A_{00}^{\vec{R}_{n-3}} = \text{rank } A_{11}^{\vec{R}_{n-3}}. \tag{58}$$

The proof for $\text{rank } B_{00}^{\vec{R}_{n-3}} = \text{rank } B_{11}^{\vec{R}_{n-3}}$ **in case** $\text{rank } A_{kk}^{\vec{R}_{n-3}} = 2$

In this section, we derive conditions on the rank of the block elements of the accumulated operators $B_{ll}^{\vec{R}_{n-3}}$ in case the rank of $A_{00}^{\vec{R}_{n-3}}$ is 2.

First, using Eqs. (28)-(40), the operators $B_{00}^{\vec{R}_{n-3}}$ and $B_{11}^{\vec{R}_{n-3}}$ defined in Eq. (17) can be rewritten as

$$B_{00}^{\vec{R}_{n-3}} = \sqrt{\sum_{r_{n-2}} |b_{00}^{(\vec{R}_{n-3},r_{n-2})}\rangle\langle b_{00}^{(\vec{R}_{n-3},r_{n-2})}|},$$

$$B_{11}^{\vec{R}_{n-3}} = \sqrt{\sum_{r_{n-2}} |b_{11}^{(\vec{R}_{n-3},r_{n-2})}\rangle\langle b_{11}^{(\vec{R}_{n-3},r_{n-2})}|},$$

and

$${}^t B_{00}^{\vec{R}_{n-3}} = B_{00}^{\vec{R}_{n-3}*} = \sqrt{\sum_{r_{n-2}} |b_{00}^{(\vec{R}_{n-3},r_{n-2})*}\rangle\langle b_{00}^{(\vec{R}_{n-3},r_{n-2})*}|} \tag{59}$$

$${}^t B_{11}^{\vec{R}_{n-3}} = B_{11}^{\vec{R}_{n-3}*} = \sqrt{\sum_{r_{n-2}} |b_{11}^{(\vec{R}_{n-3},r_{n-2})*}\rangle\langle b_{11}^{(\vec{R}_{n-3},r_{n-2})*}|}. \tag{60}$$

To proceed further, let us prove in detail the following claim which will be used several times in what follows.

Claim 2. *Given two linearly indpependent vectors $|e_1\rangle$ and $|e_2\rangle$, any two vectors $|f_1\rangle$ and $|f_2\rangle$ such that*

$$\||e_1\rangle\| = \||f_1\rangle\| \tag{61}$$
$$\||e_2\rangle\| = \||f_2\rangle\| \tag{62}$$
$$\langle e_1|e_2\rangle = e^{-i\theta}\langle f_1|f_2\rangle \tag{63}$$

must be in the form

$$|f_1\rangle = u|e_1\rangle \tag{64}$$
$$|f_2\rangle = e^{i\theta}u|e_2\rangle. \tag{65}$$

Proof. Eq. (61) implies that there exists a unitary operator u_1 such that

$$|f_1\rangle = u_1|e_1\rangle,$$

while Eq. (62) implies that there exists a unitary operator u_2 such that

$$|f_2\rangle = u_2|e_2\rangle,$$

Defining

$$u_2' = e^{-i\theta}u_2,$$

we have

$$|f_2\rangle = e^{i\theta}u_2'|e_2\rangle$$

and

$$e^{-i\theta}\langle f_1|f_2\rangle = \langle e_1|u_1^\dagger u_2'|e_2\rangle.$$

Let us define $|f_2'\rangle$ by

$$|f_2'\rangle = e^{-i\theta}|f_2\rangle.$$

Because $|e_1\rangle$ and $|e_2\rangle$ are linearly independent, there exists a linear operator T such that

$$|f_1\rangle = T|e_1\rangle \tag{66}$$
$$|f_2'\rangle = T|e_2\rangle. \tag{67}$$

Consider any $|\varphi\rangle$ given as a linear combination of $|e_1\rangle$ and $|e_2\rangle$, *i.e.*

$$|\varphi\rangle = \alpha|e_1\rangle + \beta|e_2\rangle. \tag{68}$$

Notice that Eqs. (61), (62), and (63) imply

$$\langle e_1|e_1\rangle = \langle f_1|f_1\rangle \tag{69}$$
$$\langle e_2|e_2\rangle = \langle f_2'|f_2'\rangle \tag{70}$$
$$\langle e_1|e_2\rangle = \langle f_1|f_2'\rangle. \tag{71}$$

We see that T must preserve the inner product of any two vectors of the form Eq. (68), because

$$\langle\varphi'|T^\dagger T|\varphi\rangle = (\alpha'^*\langle e_1| + \beta'^*\langle e_2|)T^\dagger \cdot T(\alpha|e_1\rangle + \beta|e_2\rangle)$$
$$= \alpha'^*\alpha\langle f_1|f_1\rangle + \alpha'^*\beta\langle f_1|f_2'\rangle$$
$$+ \beta'^*\alpha\langle f_2'|f_1\rangle + \beta'^*\beta\langle f_2'|f_2'\rangle \tag{72}$$
$$= \alpha'^*\alpha\langle e_1|e_1\rangle + \alpha'^*\beta\langle e_1|e_2\rangle$$
$$+ \beta'^*\alpha\langle e_2|e_1\rangle + \beta'^*\beta\langle e_2|e_2\rangle \tag{73}$$
$$= \langle\varphi'|\varphi\rangle. \tag{74}$$

Therefore, T is a unitary operator, which we can write as u, proving

$$|f_1\rangle = u|e_1\rangle$$
$$|f_2\rangle = e^{i\theta}u|e_2\rangle.$$

$\square$

By applying Claim 2 to Eqs. (51), (52), and (53), we see that there exists a 2×2 unitary operator $u^{\vec{R}_{n-2}}$ such that

$$A_{11}^{\vec{R}_{n-2}} X |b_{00}^{\vec{R}_{n-2}*}\rangle = u^{\vec{R}_{n-2}} A_{00}^{\vec{R}_{n-2}} X |b_{00}^{\vec{R}_{n-2}*}\rangle, \qquad (75)$$

$$A_{11}^{\vec{R}_{n-2}} X |b_{11}^{\vec{R}_{n-2}*}\rangle = e^{i\theta} u^{\vec{R}_{n-2}} A_{00}^{\vec{R}_{n-2}} X |b_{11}^{\vec{R}_{n-2}*}\rangle. \qquad (76)$$

Since the $A_{kk}^{\vec{R}_{n-2}} = A_{kk}^{\vec{R}_{n-3}}$ are full rank by hypothesis, we can define

$$T^{\vec{R}_{n-2}} = u^{\vec{R}_{n-2}\dagger} A_{11}^{\vec{R}_{n-2}} (A_{00}^{\vec{R}_{n-2}})^{-1},$$

Eqs. (75) and (76) can be transformed to

$$T^{\vec{R}_{n-2}} \cdot A_{00}^{\vec{R}_{n-2}} X |b_{00}^{\vec{R}_{n-2}*}\rangle = A_{00}^{\vec{R}_{n-2}} X |b_{00}^{\vec{R}_{n-2}*}\rangle, \qquad (77)$$

$$T^{\vec{R}_{n-2}} \cdot A_{00}^{\vec{R}_{n-2}} X |b_{11}^{\vec{R}_{n-2}*}\rangle = e^{i\theta} A_{00}^{\vec{R}_{n-2}} X |b_{11}^{\vec{R}_{n-2}*}\rangle. \qquad (78)$$

This implies that $T^{\vec{R}_{n-2}}$ has eigenvalues of 1 and $e^{i\theta}$, and corresponding eigenvectors are $A_{00}^{\vec{R}_{n-2}} X |b_{00}^{\vec{R}_{n-2}*}\rangle$ and $A_{00}^{\vec{R}_{n-2}} X |b_{11}^{\vec{R}_{n-2}*}\rangle$, respectively.

Then $T^{\vec{R}_{n-2}}$ must have the following eigen-decomposition,

$$T^{\vec{R}_{n-2}} = S^{\vec{R}_{n-2}} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} (S^{\vec{R}_{n-2}})^{-1}, \qquad (79)$$

where

$$S^{\vec{R}_{n-2}} = A_{00}^{\vec{R}_{n-2}} X |b_{00}^{\vec{R}_{n-2}*}\rangle\langle 0| + A_{00}^{\vec{R}_{n-2}} X |b_{11}^{\vec{R}_{n-2}*}\rangle\langle 1|.$$

Let us consider the singular value decomposition of $T^{\vec{R}_{n-2}}$,

$$T^{\vec{R}_{n-2}} = Q^{\vec{R}_{n-2}} \begin{pmatrix} \sqrt{\lambda_1^{\vec{R}_{n-2}}} & 0 \\ 0 & \sqrt{\lambda_2^{\vec{R}_{n-2}}} \end{pmatrix} R^{\vec{R}_{n-2}}, \qquad (80)$$

where $Q^{\vec{R}_{n-2}}$ and $R^{\vec{R}_{n-2}}$ are unitary operators and $\sqrt{\lambda_1^{\vec{R}_{n-2}}}$ and $\sqrt{\lambda_2^{\vec{R}_{n-2}}}$ are positive real numbers. Equating Eqs. (79) and (80) and taking the determinant of both sides provide us a relationship

$$\det S^{\vec{R}_{n-2}} \cdot \det \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \cdot \det(S^{\vec{R}_{n-2}})^{-1}$$

$$= \det Q^{\vec{R}_{n-2}} \cdot \det \begin{pmatrix} \sqrt{\lambda_1^{\vec{R}_{n-2}}} & 0 \\ 0 & \sqrt{\lambda_2^{\vec{R}_{n-2}}} \end{pmatrix} \cdot \det R^{\vec{R}_{n-2}}.$$

Taking the absolute value of the left hand side, we have

$$|\det S^{\vec{R}_{n-2}}| \cdot |\det \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}| \cdot |\det(S^{\vec{R}_{n-2}})^{-1}|$$

$$= |\det S^{\vec{R}_{n-2}}| \cdot |e^{i\theta}| \cdot \frac{1}{|\det(S^{\vec{R}_{n-2}})|} = 1. \qquad (81)$$

Taking the absolute value of the right hand side, recalling that the determinant of a unitary is a phase, we have

$$|\det Q^{\vec{R}_{n-2}}| \cdot |\det \begin{pmatrix} \sqrt{\lambda_1^{\vec{R}_{n-2}}} & 0 \\ 0 & \sqrt{\lambda_2^{\vec{R}_{n-2}}} \end{pmatrix}| \cdot |\det R^{\vec{R}_{n-2}}|$$

$$= 1 \cdot \sqrt{\lambda_1^{\vec{R}_{n-2}}} \sqrt{\lambda_2^{\vec{R}_{n-2}}} \cdot 1. \qquad (82)$$

Equating Eqs. (81) and (82), we obtain

$$\sqrt{\lambda_1^{\vec{R}_{n-2}}} \sqrt{\lambda_2^{\vec{R}_{n-2}}} = 1.$$

We see that the singular value decomposition of $T^{\vec{R}_{n-2}}$ is restricted to

$$T^{\vec{R}_{n-2}} = Q^{\vec{R}_{n-2}} \begin{pmatrix} \sqrt{\lambda^{\vec{R}_{n-2}}} & 0 \\ 0 & \frac{1}{\sqrt{\lambda^{\vec{R}_{n-2}}}} \end{pmatrix} R^{\vec{R}_{n-2}}.$$

We define

$$A'^{\vec{R}_{n-2}}_{00} = R^{\vec{R}_{n-2}} A_{00}^{\vec{R}_{n-2}} \qquad (83)$$

and

$$A'^{\vec{R}_{n-2}}_{11} = Q^{\vec{R}_{n-2}\dagger} u^{\vec{R}_{n-2}} A_{11}^{\vec{R}_{n-2}}. \qquad (84)$$

Using Eq.(12), let us set

$$A'^{(\vec{R}_{n-3},0)}_{00} = \tilde{A}_{00}^{\vec{R}_{n-3}} \text{ and } A'^{(\vec{R}_{n-3},0)}_{11} = \tilde{A}_{11}^{\vec{R}_{n-3}}. \qquad (85)$$

Denoting $\lambda^{(\vec{R}_{n-3},0)}$ by $\lambda^{\vec{R}_{n-3}}$, we have

$$\tilde{A}_{11}^{\vec{R}_{n-3}} = \begin{pmatrix} \sqrt{\lambda^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\lambda^{\vec{R}_{n-3}}}} \end{pmatrix} \cdot \tilde{A}_{00}^{\vec{R}_{n-3}}. \qquad (86)$$

Now the following relations hold

$$A_{00}^{(\vec{R}_{n-3},r_{n-2})\dagger} A_{00}^{(\vec{R}_{n-3},r_{n-2})} = \tilde{A}_{00}^{\vec{R}_{n-3}\dagger} \tilde{A}_{00}^{\vec{R}_{n-3}},$$

$$A_{11}^{(\vec{R}_{n-3},r_{n-2})\dagger} A_{11}^{(\vec{R}_{n-3},r_{n-2})} = \tilde{A}_{11}^{\vec{R}_{n-3}\dagger} \tilde{A}_{11}^{\vec{R}_{n-3}}.$$

We can rewrite Eqs. (51), (52), and (53) as

$$\langle b_{00}^{\vec{R}_{n-2}*}| X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger} \cdot \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{00}^{\vec{R}_{n-2}*}\rangle$$
$$= \langle b_{00}^{\vec{R}_{n-2}*}| X \tilde{A}_{11}^{\vec{R}_{n-3}\dagger} \cdot \tilde{A}_{11}^{\vec{R}_{n-3}} X |b_{00}^{\vec{R}_{n-2}*}\rangle,$$

$$\langle b_{11}^{\vec{R}_{n-2}*}| X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger} \cdot \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{11}^{\vec{R}_{n-2}*}\rangle$$
$$= \langle b_{11}^{\vec{R}_{n-2}*}| X \tilde{A}_{11}^{\vec{R}_{n-3}\dagger} \cdot \tilde{A}_{11}^{\vec{R}_{n-3}} X |b_{11}^{\vec{R}_{n-2}*}\rangle$$

and

$$\langle b_{00}^{\vec{R}_{n-2}*}| X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger} \cdot \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{11}^{\vec{R}_{n-2}*}\rangle$$
$$= e^{-i\theta} \langle b_{00}^{\vec{R}_{n-2}*}| X \tilde{A}_{11}^{\vec{R}_{n-3}\dagger} \cdot \tilde{A}_{11}^{\vec{R}_{n-3}} X |b_{11}^{\vec{R}_{n-2}*}\rangle,$$

which are equivalent to

$$\langle b_{00}^{\vec{R}_{n-2}*}|X\tilde{A}_{00}^{\vec{R}_{n-3}\dagger}\cdot\tilde{A}_{00}^{\vec{R}_{n-3}}X|b_{00}^{\vec{R}_{n-2}*}\rangle$$
$$= \langle b_{00}^{\vec{R}_{n-2}*}|X\tilde{A}_{00}^{\vec{R}_{n-3}\dagger}\cdot\begin{pmatrix}\lambda^{\vec{R}_{n-3}} & 0 \\ 0 & \frac{1}{\lambda^{\vec{R}_{n-3}}}\end{pmatrix}$$
$$\times\tilde{A}_{00}^{\vec{R}_{n-3}}X|b_{00}^{\vec{R}_{n-2}*}\rangle, \quad (87)$$

$$\langle b_{11}^{\vec{R}_{n-2}*}|X\tilde{A}_{00}^{\vec{R}_{n-3}\dagger}\cdot\tilde{A}_{00}^{\vec{R}_{n-3}}X|b_{11}^{\vec{R}_{n-2}*}\rangle$$
$$= \langle b_{11}^{\vec{R}_{n-2}*}|X\tilde{A}_{00}^{\vec{R}_{n-3}\dagger}\cdot\begin{pmatrix}\lambda^{\vec{R}_{n-3}} & 0 \\ 0 & \frac{1}{\lambda^{\vec{R}_{n-3}}}\end{pmatrix}$$
$$\times\tilde{A}_{00}^{\vec{R}_{n-3}}X|b_{11}^{\vec{R}_{n-2}*}\rangle, \quad (88)$$

and

$$\langle b_{00}^{\vec{R}_{n-2}*}|X\tilde{A}_{00}^{\vec{R}_{n-3}\dagger}\cdot\tilde{A}_{00}^{\vec{R}_{n-3}}X|b_{11}^{\vec{R}_{n-2}*}\rangle$$
$$= e^{-i\theta}\langle b_{00}^{\vec{R}_{n-2}*}|X\tilde{A}_{00}^{\vec{R}_{n-3}\dagger}\cdot\begin{pmatrix}\lambda^{\vec{R}_{n-3}} & 0 \\ 0 & \frac{1}{\lambda^{\vec{R}_{n-3}}}\end{pmatrix}$$
$$\times\tilde{A}_{00}^{\vec{R}_{n-3}}X|b_{11}^{\vec{R}_{n-2}*}\rangle. \quad (89)$$

We now consider two cases, namely, when $\lambda^{\vec{R}_{n-3}} \neq 1$ and $\lambda^{\vec{R}_{n-3}} = 1$, and prove that rank $B_{00}^{\vec{R}_{n-3}} = $ rank $B_{11}^{\vec{R}_{n-3}}$ holds for each case.

The $\lambda^{\vec{R}_{n-3}} \neq 1$ case

We consider the case of $\lambda^{\vec{R}_{n-3}} \neq 1$. Let us define the coefficients of $\tilde{A}_{00}^{\vec{R}_{n-3}}X|b_{00}^{\vec{R}_{n-2}*}\rangle$ and $\tilde{A}_{00}^{\vec{R}_{n-3}}X|b_{11}^{\vec{R}_{n-2}*}\rangle$ by

$$\tilde{A}_{00}^{\vec{R}_{n-3}}X|b_{00}^{\vec{R}_{n-2}*}\rangle = a_0^{\vec{R}_{n-2}}e^{i\omega_{00}^{\vec{R}_{n-2}}}|0\rangle + b_0^{\vec{R}_{n-2}}e^{i\omega_{01}^{\vec{R}_{n-2}}}|1\rangle$$
$$\tilde{A}_{00}^{\vec{R}_{n-3}}X|b_{11}^{\vec{R}_{n-2}*}\rangle = a_1^{\vec{R}_{n-2}}e^{i\omega_{10}^{\vec{R}_{n-2}}}|0\rangle + b_1^{\vec{R}_{n-2}}e^{i\omega_{11}^{\vec{R}_{n-2}}}|1\rangle,$$

where $a_0^{\vec{R}_{n-2}}, a_1^{\vec{R}_{n-2}}, b_0^{\vec{R}_{n-2}}, b_1^{\vec{R}_{n-2}}, \omega_{00}^{\vec{R}_{n-2}}, \omega_{01}^{\vec{R}_{n-2}}, \omega_{10}^{\vec{R}_{n-2}},$ and $\omega_{11}^{\vec{R}_{n-2}}$ are all real numbers. With this notation, Eqs. (87), (88), and (89) read

$$(a_0^{\vec{R}_{n-2}})^2 + (b_0^{\vec{R}_{n-2}})^2$$
$$= \lambda^{\vec{R}_{n-3}}(a_0^{\vec{R}_{n-2}})^2 + \frac{1}{\lambda^{\vec{R}_{n-3}}}(b_0^{\vec{R}_{n-2}})^2, \quad (90)$$

$$(a_1^{\vec{R}_{n-2}})^2 + (b_1^{\vec{R}_{n-2}})^2$$
$$= \lambda^{\vec{R}_{n-3}}(a_1^{\vec{R}_{n-2}})^2 + \frac{1}{\lambda^{\vec{R}_{n-3}}}(b_1^{\vec{R}_{n-2}})^2, \quad (91)$$

and

$$a_0^{\vec{R}_{n-2}}a_1^{\vec{R}_{n-2}}e^{i(\omega_{00}^{\vec{R}_{n-2}}-\omega_{10}^{\vec{R}_{n-2}})}$$
$$+ b_0^{\vec{R}_{n-2}}b_1^{\vec{R}_{n-2}}e^{i(\omega_{01}^{\vec{R}_{n-2}}-\omega_{11}^{\vec{R}_{n-2}})}$$
$$= e^{-i\theta}(\lambda^{\vec{R}_{n-3}}a_0^{\vec{R}_{n-2}}a_1^{\vec{R}_{n-2}}e^{i(\omega_{00}^{\vec{R}_{n-2}}-\omega_{10}^{\vec{R}_{n-2}})}$$
$$+ \frac{1}{\lambda^{\vec{R}_{n-3}}}b_0^{\vec{R}_{n-2}}b_1^{\vec{R}_{n-2}}e^{i(\omega_{10}^{\vec{R}_{n-2}}-\omega_{11}^{\vec{R}_{n-2}})}). \quad (92)$$

Eq. (54) becomes

$$(a_0^{\vec{R}_{n-2}})^2 + (b_0^{\vec{R}_{n-2}})^2 = (a_1^{\vec{R}_{n-2}})^2 + (b_1^{\vec{R}_{n-2}})^2. \quad (93)$$

Eqs. (90) and (91) imply that

$$\frac{(a_0^{\vec{R}_{n-2}})^2}{(b_0^{\vec{R}_{n-2}})^2} = \frac{\frac{1}{\lambda^{\vec{R}_{n-3}}}-1}{1-\lambda^{\vec{R}_{n-3}}} = \frac{1}{\lambda^{\vec{R}_{n-3}}} = \frac{(a_1^{\vec{R}_{n-2}})^2}{(b_1^{\vec{R}_{n-2}})^2}, \quad (94)$$

where the assumption $\lambda^{\vec{R}_{n-3}} \neq 1$ guarantees that the quotient is well defined. The last two equations imply that

$$a_0^{\vec{R}_{n-2}} = a_1^{\vec{R}_{n-2}} \text{ and } b_0^{\vec{R}_{n-2}} = b_1^{\vec{R}_{n-2}}. \quad (95)$$

We divide both sides of Eq. (92) by $b_0^{\vec{R}_{n-2}}b_1^{\vec{R}_{n-2}}e^{i(\omega_{01}^{\vec{R}_{n-2}}-\omega_{11}^{\vec{R}_{n-2}})}$ and use Eqs. (94) and (95) to derive

$$\frac{1}{\lambda^{\vec{R}_{n-3}}}\cdot e^{-i\delta^{\vec{R}_{n-2}}} + 1 = e^{-i\theta}(e^{-i\delta^{\vec{R}_{n-2}}} + \frac{1}{\lambda^{\vec{R}_{n-3}}})$$
$$\iff \lambda^{\vec{R}_{n-3}} + e^{-i\delta^{\vec{R}_{n-2}}} = e^{-i\theta}(1 + \lambda^{\vec{R}_{n-3}}\cdot e^{-i\delta^{\vec{R}_{n-2}}}),$$
$$(96)$$

where

$$\delta^{\vec{R}_{n-2}} = \omega_{01}^{\vec{R}_{n-2}} - \omega_{11}^{\vec{R}_{n-2}} - \omega_{00}^{\vec{R}_{n-2}} + \omega_{10}^{\vec{R}_{n-2}}.$$

Eq. (96) is equivalent to

$$e^{-i\delta^{\vec{R}_{n-2}}} = \frac{\lambda^{\vec{R}_{n-3}} - e^{-i\theta}}{\lambda^{\vec{R}_{n-3}}e^{-i\theta} - 1}, \quad (97)$$

which implies independence of r_{n-2}:

$$e^{-i\delta^{(\vec{R}_{n-3},0)}} = e^{-i\delta^{(\vec{R}_{n-3},r_{n-2})}}.$$

By defining

$$\delta^{\vec{R}_{n-3}} = \delta^{(\vec{R}_{n-3},0)} \text{ and } \Delta^{\vec{R}_{n-2}} = \omega_{01}^{\vec{R}_{n-2}} - \omega_{00}^{\vec{R}_{n-2}}$$

and using Eqs. (94) and (95), we obtain

$$\tilde{A}_{00}^{\vec{R}_{n-3}}X|b_{00}^{\vec{R}_{n-2}*}\rangle$$
$$= a_0^{\vec{R}_{n-2}}e^{i\omega_{00}^{\vec{R}_{n-2}}}(|0\rangle + \sqrt{\lambda^{\vec{R}_{n-3}}}e^{i\Delta^{\vec{R}_{n-2}}}|1\rangle)$$

and

$$\tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{11}^{\vec{R}_{n-2}*}\rangle$$
$$= a_0^{\vec{R}_{n-2}} e^{i\omega_{10}^{\vec{R}_{n-2}}} (|0\rangle + \sqrt{\lambda^{\vec{R}_{n-3}}} e^{i(\Delta^{\vec{R}_{n-2}} - \delta^{\vec{R}_{n-2}})} |1\rangle).$$

Introducing

$$c_0^{\vec{R}_{n-3}} = a_0^{\vec{R}_{n-2}} e^{i\omega_{00}^{\vec{R}_{n-2}}} \text{ and } c_1^{\vec{R}_{n-3}} = a_0^{\vec{R}_{n-2}} e^{i\omega_{10}^{\vec{R}_{n-2}}},$$

we can write these relations as

$$\tilde{A}_{kk}^{\vec{R}_{n-3}} X |b_{ll}^{\vec{R}_{n-2}*}\rangle = c_l^{\vec{R}_{n-3}} \cdot \begin{pmatrix} \sqrt{\lambda^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\lambda^{\vec{R}_{n-3}}}} \end{pmatrix}^k$$
$$\times \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\delta^{\vec{R}_{n-3}}} \end{pmatrix}^l \cdot (|0\rangle + \sqrt{\lambda^{\vec{R}_{n-3}}} e^{i\Delta^{\vec{R}_{n-2}}} |1\rangle).$$

For any $k, l, k', l' \in \{0, 1\}$ the following holds

$$\text{Tr} \tilde{A}_{kk}^{\vec{R}_{n-3}} X |b_{ll}^{\vec{R}_{n-2}*}\rangle\langle b_{ll}^{\vec{R}_{n-2}*}| X \tilde{A}_{kk}^{\vec{R}_{n-3}\dagger}$$
$$= \text{Tr} A_{k'k'}^{\vec{R}_{n-3}} X |b_{l'l'}^{\vec{R}_{n-2}*}\rangle\langle b_{l'l'}^{\vec{R}_{n-2}*}| X A_{k'k'}^{\vec{R}_{n-3}\dagger}. \quad (98)$$

This gives

$$\tilde{A}_{00}^{\vec{R}_{n-3}} X {}^t B_{11}^{\vec{R}_{n-3}} B_{11}^{\vec{R}_{n-3}*} X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}$$
$$= \sum_{r_{n-2}} \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{11}^{(\vec{R}_{n-3},r_{n-2})*}\rangle\langle b_{11}^{(\vec{R}_{n-3},r_{n-2})*}| X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}$$
$$= \sum_{r_{n-2}} \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\delta^{\vec{R}_{n-3}}} \end{pmatrix} \cdot \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{11}^{(\vec{R}_{n-3},r_{n-2})*}\rangle \times (c.c.)$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\delta^{\vec{R}_{n-3}}} \end{pmatrix} \cdot \tilde{A}_{00}^{\vec{R}_{n-3}} X {}^t B_{00}^{\vec{R}_{n-3}} \times (c.c.). \quad (99)$$

Note that $\tilde{A}_{00}^{\vec{R}_{n-3}}$, $\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\delta^{\vec{R}_{n-3}}} \end{pmatrix}$, and X are all full rank, implying that their determinants are nonzero. Taking the determinant of both sides, we obtain

$$\det {}^t B_{00}^{\vec{R}_{n-3}} B_{00}^{\vec{R}_{n-3}*} = \det {}^t B_{11}^{\vec{R}_{n-3}} B_{11}^{\vec{R}_{n-3}*} \quad (100)$$

Because $B_{00}^{\vec{R}_{n-3}}$ and $B_{11}^{\vec{R}_{n-3}}$ are 2×2 nonzero matrices, if the rank of $B_{00}^{\vec{R}_{n-3}}$ is one, then the left hand side of Eq. (100) is zero and thus the rank of $B_{00}^{\vec{R}_{n-3}}$ is also one. On the other hand, if $B_{00}^{\vec{R}_{n-3}}$ is full rank, then so is $B_{00}^{\vec{R}_{n-3}}$. Therefore, we have that for any successful LOCC implementaion protocol,

$$\text{rank } B_{00}^{\vec{R}_{n-3}} = \text{rank } B_{11}^{\vec{R}_{n-3}} \quad (101)$$

for $\lambda^{\vec{R}_{n-3}} \neq 1$.

The $\lambda^{\vec{R}_{n-3}} = 1$ case

Next, we consider the case when $\lambda^{\vec{R}_{n-3}} = 1$. Notice that this means that $A_{11}^{\vec{R}_{n-3}} (A_{00}^{\vec{R}_{n-3}})^{-1}$ is a unitary operation, which is exactly the assumption of Lemma 4. By Eq.(86), we have

$$\tilde{A}_{11}^{\vec{R}_{n-3}} = \tilde{A}_{00}^{\vec{R}_{n-3}}. \quad (102)$$

Eq. (89) implies

$$\langle b_{00}^{\vec{R}_{n-2}*}| X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger} \cdot \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{11}^{\vec{R}_{n-2}*}\rangle$$
$$= e^{-i\theta} \langle b_{00}^{\vec{R}_{n-2}*}| X \tilde{A}_{11}^{\vec{R}_{n-3}\dagger} \cdot \tilde{A}_{11}^{\vec{R}_{n-3}} X |b_{11}^{\vec{R}_{n-2}*}\rangle$$
$$= e^{-i\theta} \langle b_{00}^{\vec{R}_{n-2}*}| X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger} \cdot \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{11}^{\vec{R}_{n-2}*}\rangle.$$

Because $e^{-i\theta} \neq 1$, the last equation forces

$$\langle b_{00}^{\vec{R}_{n-2}*}| X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger} \cdot \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{11}^{\vec{R}_{n-2}*}\rangle = 0. \quad (103)$$

We define $|g^{\vec{R}_{n-2}}\rangle$ and $|g^{\vec{R}_{n-2}\perp}\rangle$ by

$$|g^{\vec{R}_{n-2}}\rangle = \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{00}^{\vec{R}_{n-2}*}\rangle,$$
$$|g^{\vec{R}_{n-2}\perp}\rangle = \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{11}^{\vec{R}_{n-2}*}\rangle.$$

By Eqs. (54) and (103), we have

$$\| |g^{\vec{R}_{n-2}}\rangle \| = \| |g^{\vec{R}_{n-2}}\rangle \| \equiv C^{\vec{R}_{n-2}}$$

and

$$\langle g^{\vec{R}_{n-2}} | g^{\vec{R}_{n-2}\perp}\rangle = 0.$$

Because $|g^{\vec{R}_{n-2}}\rangle$ and $|g^{\vec{R}_{n-2}\perp}\rangle$ are two-dimensional vectors,

$$|g^{\vec{R}_{n-2}}\rangle\langle g^{\vec{R}_{n-2}}| + |g^{\vec{R}_{n-2}\perp}\rangle\langle g^{\vec{R}_{n-2}\perp}| = \mathbb{I}_2,$$

where $\mathbb{I}_2$ is the 2×2 identity matrix.

Next, we obtain the following relation

$$\tilde{A}_{00}^{\vec{R}_{n-3}} X {}^t B_{00}^{\vec{R}_{n-3}} B_{00}^{\vec{R}_{n-3}*} X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}$$
$$+ \tilde{A}_{00}^{\vec{R}_{n-3}} X {}^t B_{11}^{\vec{R}_{n-3}} B_{11}^{\vec{R}_{n-3}*} X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}$$
$$= \sum_{r_{n-2}} \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{00}^{\vec{R}_{n-2}*}\rangle\langle b_{00}^{\vec{R}_{n-2}*}| X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}$$
$$+ \tilde{A}_{00}^{\vec{R}_{n-3}} X |b_{11}^{\vec{R}_{n-2}*}\rangle\langle b_{11}^{\vec{R}_{n-2}*}| X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}$$
$$= \sum_{r_{n-2}} |g^{\vec{R}_{n-2}}\rangle\langle g^{\vec{R}_{n-2}}| + |g^{\vec{R}_{n-2}\perp}\rangle\langle g^{\vec{R}_{n-2}\perp}|$$
$$= \left[\sum_{r_{n-2}} (C^{(\vec{R}_{n-3},r_{n-2})})^2 \right] \cdot \mathbb{I}_2, \quad (104)$$

where we have used Eqs. (59) and (60). Thus one sees that

$$\tilde{A}_{00}^{\vec{R}_{n-3}} X {}^t B_{00}^{\vec{R}_{n-3}} B_{00}^{\vec{R}_{n-3}*} X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}$$

and

$$\tilde{A}_{00}^{\vec{R}_{n-3}} X^t B_{11}^{\vec{R}_{n-3}} B_{11}^{\vec{R}_{n-3}*} X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}$$

commute, and are therefore simultaneously diagonalizable:

$$\tilde{A}_{00}^{\vec{R}_{n-3}} X^t B_{00}^{\vec{R}_{n-3}} B_{00}^{\vec{R}_{n-3}*} X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}$$
$$= V^{\vec{R}_{n-3}} \begin{pmatrix} e_0^{\vec{R}_{n-3}} & \\ & f_0^{\vec{R}_{n-3}} \end{pmatrix} V^{\vec{R}_{n-3}\dagger},$$

and

$$\tilde{A}_{00}^{\vec{R}_{n-3}} X^t B_{11}^{\vec{R}_{n-3}} B_{11}^{\vec{R}_{n-3}*} X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}$$
$$= V^{\vec{R}_{n-3}} \begin{pmatrix} e_1^{\vec{R}_{n-3}} & \\ & f_1^{\vec{R}_{n-3}} \end{pmatrix} V^{\vec{R}_{n-3}\dagger}.$$

Also we note that

$$\mathrm{Tr}\,\tilde{A}_{00}^{\vec{R}_{n-3}} X^t B_{00}^{\vec{R}_{n-3}} B_{00}^{\vec{R}_{n-3}*} X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}$$
$$= \sum_{r_{n-2}} \mathrm{Tr}\,|g^{(\vec{R}_{n-3}, r_{n-2})}\rangle\langle g^{(\vec{R}_{n-3}, r_{n-2})}|$$
$$= \sum_{r_{n-2}} \||g^{(\vec{R}_{n-3}, r_{n-2})}\rangle\|^2$$
$$= \sum_{r_{n-2}} \||g^{(\vec{R}_{n-3}, r_{n-2})\perp}\rangle\|^2$$
$$= \sum_{r_{n-2}} \mathrm{Tr}\,|g^{(\vec{R}_{n-3}, r_{n-2})\perp}\rangle\langle g^{(\vec{R}_{n-3}, r_{n-2})\perp}|$$
$$= \mathrm{Tr}\,\tilde{A}_{00}^{\vec{R}_{n-3}} X^t B_{11}^{\vec{R}_{n-3}} B_{11}^{\vec{R}_{n-3}*} X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}. \quad (105)$$

Eq. (104) implies that

$$e_0^{\vec{R}_{n-3}} + e_1^{\vec{R}_{n-3}} = f_0^{\vec{R}_{n-3}} + f_1^{\vec{R}_{n-3}},$$

while Eq. (105) implies

$$e_0^{\vec{R}_{n-3}} + f_0^{\vec{R}_{n-3}} = e_1^{\vec{R}_{n-3}} + f_1^{\vec{R}_{n-3}}.$$

Comparing the two equations, we obtain

$$e_0^{\vec{R}_{n-3}} = f_1^{\vec{R}_{n-3}}$$
$$e_1^{\vec{R}_{n-3}} = f_0^{\vec{R}_{n-3}}.$$

The last two equations imply that

$$\mathrm{rank}\,B_{00}^{\vec{R}_{n-3}} = \mathrm{rank}\,B_{11}^{\vec{R}_{n-3}}, \quad (106)$$

completing the proof.

Proof of Lemma 2

In this section we provide the proof for Lemma 2. We begin with case (a).

As discussed in the proof of Lemma 1, $\langle a_{kk}^{(\vec{R}_{n-2}, r_{n-1}, r_n)}|$ does not have any r_n-dependence, which implies that

$$A_{kk}^{\vec{R}_{n-3}} = \sqrt{\sum_{r_{n-1}} |a_{kk}^{(\vec{R}_{n-3}, r_{n-2}, r_{n-1}, 0)}\rangle\langle a_{kk}^{(\vec{R}_{n-3}, r_{n-2}, r_{n-1}, 0)}|}.$$

For this to be rank 1, there must exist complex numbers $\gamma'_0{}^{(\vec{R}_{n-2}, r_{n-1})}$ and $\gamma'_0{}^{(\vec{R}_{n-2}, r_{n-1})}$ such that

$$\langle a_{00}^{(\vec{R}_{n-2}, r_{n-1}, 0)}| = \gamma'_0{}^{(\vec{R}_{n-2}, r_{n-1})} \langle a_{00}^{(\vec{R}_{n-2}, 0, 0)}|$$
$$\langle a_{11}^{(\vec{R}_{n-2}, r_{n-1}, 0)}| = \gamma'_1{}^{(\vec{R}_{n-2}, r_{n-1})} \langle a_{11}^{(\vec{R}_{n-2}, 0, 0)}|.$$

By Eq. (51), we see that

$$|\gamma'_0{}^{(\vec{R}_{n-2}, r_{n-1})}| = |\gamma'_1{}^{(\vec{R}_{n-2}, r_{n-1})}|,$$

hence $\gamma'_0{}^{(\vec{R}_{n-2}, r_{n-1})}$ and $\gamma'_1{}^{(\vec{R}_{n-2}, r_{n-1})}$ can be rewritten as

$$\gamma'_0{}^{(\vec{R}_{n-2}, r_{n-1})} = |\gamma'_0{}^{(\vec{R}_{n-2}, r_{n-1})}| \exp(i \arg \gamma'_0{}^{(\vec{R}_{n-2}, r_{n-1})}) \quad (107)$$
$$\gamma'_1{}^{(\vec{R}_{n-2}, r_{n-1})} = |\gamma'_0{}^{(\vec{R}_{n-2}, r_{n-1})}| \exp(i \arg \gamma'_1{}^{(\vec{R}_{n-2}, r_{n-1})}). \quad (108)$$

Defining a positive number

$$g'^{\vec{R}_{n-2}} = \sqrt{\sum_{r_{n-1}} |\gamma'_0{}^{(\vec{R}_{n-2}, r_{n-1})}|^2},$$

it is easy to see by Eqs. (12) and (18) that

$$A^{\vec{R}_{n-2}\dagger} A^{\vec{R}_{n-2}}$$
$$= (g'^{\vec{R}_{n-2}})^2 \cdot (|0\rangle\langle 0| \otimes |a_{00}^{(\vec{R}_{n-2}, 0, 0)}\rangle\langle a_{00}^{(\vec{R}_{n-2}, 0, 0)}|$$
$$+ |1\rangle\langle 1| \otimes |a_{11}^{(\vec{R}_{n-2}, 0, 0)}\rangle\langle a_{11}^{(\vec{R}_{n-2}, 0, 0)}|).$$

Therefore, by Claim 1, there exists an isometry $U_A^{\vec{R}_{n-2}}$ such that

$$A^{\vec{R}_{n-2}} = U_A^{\vec{R}_{n-2}} \cdot (|0\rangle\langle 0| \otimes g'^{\vec{R}_{n-2}} \langle a_{00}^{(\vec{R}_{n-2}, 0)}|$$
$$+ |1\rangle\langle 1| \otimes g'^{\vec{R}_{n-2}} \langle a_{11}^{(\vec{R}_{n-2}, 0)}|). \quad (109)$$

Using Eqs. (25), (26), and (27), it can be checked by direct calculation that the random unitary operation $\{p^{\vec{R}_{n-1}}, U^{\vec{R}_{n-1}}\}$ in question is given by

$$p^{\vec{R}_{n-1}} = \frac{|\gamma'_0{}^{(\vec{R}_{n-2}, r_{n-1})}|^2}{(g'^{\vec{R}_{n-2}})^2}$$

and

$$U^{\vec{R}_{n-1}} = \begin{pmatrix} \exp(i\arg\gamma'^{\vec{R}_{n-1}}_0) & 0 \\ 0 & \exp(i\arg\gamma'^{\vec{R}_{n-1}}_1) \end{pmatrix} \cdot U_A^{\vec{R}_{n-2}\dagger}.$$

Next, we proceed to case (b). In Eq. (14), the left hand side is independent of r_{n-1} therefore the right hand should also be independent of r_{n-1} and we set

$$B^{\vec{R}_{n-2}} = B^{(\vec{R}_{n-2},0)}.$$

By Eq. (15) we have

$$B^{\vec{R}_{n-3}\dagger}B^{\vec{R}_{n-3}} = \sum_{r_{n-2}} B^{\vec{R}_{n-1}\dagger}B^{\vec{R}_{n-1}}. \tag{110}$$

Combined with Eqs. (36) and (37), we obtain

$$B^{\vec{R}_{n-3}}_{ll} = \sqrt{\sum_{r_{n-2}} |b^{(\vec{R}_{n-2},0)}_{ll}\rangle\langle b^{(\vec{R}_{n-2},0)}_{ll}|}.$$

Because $B^{\vec{R}_{n-3}}_{00}$ and $B^{\vec{R}_{n-3}}_{11}$ are both rank 1 by assumption, there exist two complex numbers $\gamma''^{(\vec{R}_{n-3},r_{n-2})}_0$ and $\gamma''^{(\vec{R}_{n-3},r_{n-2})}_1$ such that

$$\langle b^{(\vec{R}_{n-2},0)}_{00}| = \gamma''^{(\vec{R}_{n-3},r_{n-2})}_0 \langle b^{(\vec{R}_{n-3},0,0)}_{00}|$$
$$\langle b^{(\vec{R}_{n-2},0)}_{11}| = \gamma''^{(\vec{R}_{n-3},r_{n-2})}_1 \langle b^{(\vec{R}_{n-3},0,0)}_{11}|.$$

By Eq. (54), we see that

$$|\gamma''^{(\vec{R}_{n-3},r_{n-2})}_0| = |\gamma''^{(\vec{R}_{n-3},r_{n-2})}_1|.$$

Defining a positive number

$$g''^{\vec{R}_{n-3}} = \sqrt{\sum_{r_{n-2}} |\gamma''^{(\vec{R}_{n-3},r_{n-2})}_0|^2},$$

it is easy to see that

$$B^{\vec{R}_{n-3}\dagger}B^{\vec{R}_{n-3}} = (g''^{\vec{R}_{n-3}})^2$$
$$\times (|0\rangle\langle 0| \otimes |b^{(\vec{R}_{n-3},0,0)}_{00}\rangle\langle b^{(\vec{R}_{n-3},0,0)}_{00}|$$
$$+ |1\rangle\langle 1| \otimes |b^{(\vec{R}_{n-3},0,0)}_{11}\rangle\langle b^{(\vec{R}_{n-3},0,0)}_{11}|).$$

Therefore, there exists an isometry $U_B^{\vec{R}_{n-3}}$ by Claim 1 such that

$$B^{\vec{R}_{n-3}} = U_B^{\vec{R}_{n-3}} \cdot (|0\rangle\langle 0| \otimes g''^{\vec{R}_{n-3}}\langle b^{(\vec{R}_{n-3},0)}_{00}|$$
$$+ |1\rangle\langle 1| \otimes g''^{\vec{R}_{n-3}}\langle b^{(\vec{R}_{n-3},0)}_{11}|).$$

It can be checked by direct calculation that the random unitary operation $\{q^{\vec{R}_{n-2}}, V^{\vec{R}_{n-2}}\}$ in question is given by

$$q^{\vec{R}_{n-2}} = \frac{|\gamma''^{\vec{R}_{n-2}}_0|^2}{(g''^{\vec{R}_{n-3}})^2}$$

and

$$V^{\vec{R}_{n-2}} = \begin{pmatrix} \exp(i\arg\gamma''^{\vec{R}_{n-2}}_0) & 0 \\ 0 & \exp(i\arg\gamma''^{\vec{R}_{n-2}}_1) \end{pmatrix} \cdot U_B^{\vec{R}_{n-3}\dagger}.$$

Proof of Lemma 3

In this section we present the proof for Lemma 3. The proof requires the following claim, which will also be proven in this section.

Let us define

$$E_{kl} = \tilde{A}^{\vec{R}_{n-3}}_{kk} X^t B'^{\vec{R}_{n-3}}_{ll}.$$

Claim 3. *When $A^{\vec{R}_{n-3}}_{00}$ and $B^{\vec{R}_{n-3}}_{00}$ are both rank 2 in a successful protocol, then the accumulated operators $A^{\vec{R}_{n-3}}$ and $B^{\vec{R}_{n-3}}$ can be expressed as follows*

$$A^{\vec{R}_{n-3}} = U_A^{\vec{R}_{n-3}} \cdot (|0\rangle\langle 0| \otimes E_{00}({}^t B'^{\vec{R}_{n-3}}_{00})^{-1}X^{-1}$$
$$+ |1\rangle\langle 1| \otimes E_{00} \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\delta'^{\vec{R}_{n-3}}} \end{pmatrix} ({}^t B'^{\vec{R}_{n-3}}_{00})^{-1}X^{-1}, \tag{111}$$

and

$$B^{\vec{R}_{n-3}} = U_B^{\vec{R}_{n-3}}(|0\rangle\langle 0| \otimes B'^{\vec{R}_{n-3}}_{00}$$
$$+ |1\rangle\langle 1| \otimes \begin{pmatrix} \sqrt{\mu^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\mu^{\vec{R}_{n-3}}}} \end{pmatrix} B'^{\vec{R}_{n-3}}_{00}) \tag{112}$$

where $\mu^{\vec{R}_{n-3}}$ and $\delta'^{\vec{R}_{n-3}}$ satisfy

$$\mu^{\vec{R}_{n-3}} + e^{-i\delta'^{\vec{R}_{n-3}}} = e^{i\theta}(1 + \mu^{\vec{R}_{n-3}}e^{-i\delta'^{\vec{R}_{n-3}}}). \tag{113}$$

Moreoever, there exist phase factors $e^{i\varphi_0}$ and $e^{i\varphi_1}$ such that

$$E^{\vec{R}_{n-3}\dagger}_{00}E^{\vec{R}_{n-3}}_{00} = \frac{|e_{00}|^2(1 + \mu^{\vec{R}_{n-3}})}{2} \times$$
$$\left[\sum_{l=0,1}(|0\rangle + \sqrt{\mu^{\vec{R}_{n-3}}}e^{-i\varphi_l}|1\rangle)(\langle 0| + \sqrt{\mu^{\vec{R}_{n-3}}}e^{i\varphi_l}\langle 1|)\right]. \tag{114}$$

Proof. As in the proof of lemma 1, we divide the proof for the cases where $\lambda^{\vec{R}_{n-3}} \neq 1$ and $\lambda^{\vec{R}_{n-3}} = 1$, and start with the former. Defining

$$T_B^{\vec{R}_{n-3}} = B^{\vec{R}_{n-3}*}_{11}(B^{\vec{R}_{n-3}*}_{00})^{-1},$$

Eq. (100) is equivalent to

$$\det {}^t B^{\vec{R}_{n-3}}_{00}B^{\vec{R}_{n-3}*}_{00} = \det {}^t B^{\vec{R}_{n-3}}_{00} \cdot T_B^{\vec{R}_{n-3}\dagger}T_B^{\vec{R}_{n-3}} \cdot B^{\vec{R}_{n-3}*}_{00}. \tag{115}$$

By hypothesis, $\det B^{\vec{R}_{n-3}}_{00}$ is nonzero. Thus dividing Eq. (115) by $\det B^{\vec{R}_{n-3}*}_{00}$ and $\det {}^t B^{\vec{R}_{n-3}}_{00}$, we have

$$1 = \det T_B^{\vec{R}_{n-3}\dagger}T_B^{\vec{R}_{n-3}}. \tag{116}$$

Denoting the singular value decomposition of $T_B^{\vec{R}_{n-3}}$ by

$$T_B^{\vec{R}_{n-3}} = Q_B^{\vec{R}_{n-3}} \begin{pmatrix} \sqrt{\mu_1^{\vec{R}_{n-3}}} & 0 \\ 0 & \sqrt{\mu_2^{\vec{R}_{n-3}}} \end{pmatrix} R_B^{\vec{R}_{n-3}},$$

Eq. (116) implies that

$$1 = \mu_1^{\vec{R}_{n-3}} \mu_2^{\vec{R}_{n-3}},$$

which restricts the singular value decomposition of $T_B^{\vec{R}_{n-3}}$ to be

$$T_B^{\vec{R}_{n-3}} = Q_B^{\vec{R}_{n-3}} \begin{pmatrix} \sqrt{\mu^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\mu^{\vec{R}_{n-3}}}} \end{pmatrix} R_B^{\vec{R}_{n-3}}.$$

Let us define

$$B'^{\vec{R}_{n-3}}_{00} = R_B^{\vec{R}_{n-3}*} B^{\vec{R}_{n-3}}_{00} \text{ and } B'^{\vec{R}_{n-3}}_{11} = {}^t Q^{\vec{R}_{n-3}} B^{\vec{R}_{n-3}}_{11}. \tag{117}$$

Recalling the definition of $T_B^{\vec{R}_{n-3}}$, $B'^{\vec{R}_{n-3}}_{00}$ and $B'^{\vec{R}_{n-3}}_{11}$ have to satisfy

$$B'^{\vec{R}_{n-3}}_{11} = \begin{pmatrix} \sqrt{\mu^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\mu^{\vec{R}_{n-3}}}} \end{pmatrix} B'^{\vec{R}_{n-3}}_{00}. \tag{118}$$

For any $k,l,k',l' \in \{0,1\}$, Eq. (98) implies that

$$\mathrm{Tr}\, \tilde{A}_{kk}^{\vec{R}_{n-3}} X^t B_{ll}^{\vec{R}_{n-3}} B_{ll}^{\vec{R}_{n-3}*} X \tilde{A}_{kk}^{\vec{R}_{n-3}\dagger}$$
$$= \mathrm{Tr}\, A_{k'k'}^{\vec{R}_{n-3}} X^t B_{l'l'}^{\vec{R}_{n-3}} B_{l'l'}^{\vec{R}_{n-3}*} X A_{k'k'}^{\vec{R}_{n-3}\dagger}.$$

Using this relation, we have that

$$\mathrm{Tr}\, \tilde{A}_{kk}^{\vec{R}_{n-3}} X^t B'^{\vec{R}_{n-3}}_{ll} B'^{\vec{R}_{n-3}*}_{ll} X \tilde{A}_{kk}^{\vec{R}_{n-3}\dagger}$$
$$= \mathrm{Tr}\, \tilde{A}_{kk}^{\vec{R}_{n-3}} X^t B_{ll}^{\vec{R}_{n-3}} B_{ll}^{\vec{R}_{n-3}*} X \tilde{A}_{kk}^{\vec{R}_{n-3}\dagger}$$
$$= \mathrm{Tr}\, A_{k'k'}^{\vec{R}_{n-3}} X^t B_{l'l'}^{\vec{R}_{n-3}} B_{l'l'}^{\vec{R}_{n-3}*} X A_{k'k'}^{\vec{R}_{n-3}\dagger}$$
$$= \mathrm{Tr}\, A_{k'k'}^{\vec{R}_{n-3}} X^t B'^{\vec{R}_{n-3}}_{l'l'} B'^{\vec{R}_{n-3}*}_{l'l'} X A_{k'k'}^{\vec{R}_{n-3}\dagger}. \tag{119}$$

Eqs. (86) and (118) show that $\det \tilde{A}_{kk}^{\vec{R}_{n-3}}$ and $\det B'^{\vec{R}_{n-3}}_{kk}$ are independent of k, and so

$$\det(\tilde{A}_{kk}^{\vec{R}_{n-3}} X^t B'^{\vec{R}_{n-3}}_{ll} B'^{\vec{R}_{n-3}*}_{ll} X \tilde{A}_{kk}^{\vec{R}_{n-3}\dagger})$$
$$= \det(\tilde{A}_{00}^{\vec{R}_{n-3}} X^t B'^{\vec{R}_{n-3}}_{00} B'^{\vec{R}_{n-3}*}_{00} X \tilde{A}_{00}^{\vec{R}_{n-3}\dagger}). \tag{120}$$

Eqs. (86) and (118) imply

$$E_{kl} = \begin{pmatrix} \sqrt{\lambda^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\lambda^{\vec{R}_{n-3}}}} \end{pmatrix}^k \cdot E_{00} \cdot \begin{pmatrix} \sqrt{\mu^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\mu^{\vec{R}_{n-3}}}} \end{pmatrix}^l. \tag{121}$$

By choosing $(k,l) = (0,0)$ and $(k',l') = (1,0)$ in Eq. (119), we have

$$\mathrm{Tr}\, E_{00} E_{00}^{\dagger} = \mathrm{Tr} \begin{pmatrix} \sqrt{\lambda^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\lambda^{\vec{R}_{n-3}}}} \end{pmatrix} \cdot E_{00} E_{00}^{\dagger}$$
$$\cdot \begin{pmatrix} \sqrt{\lambda^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\lambda^{\vec{R}_{n-3}}}} \end{pmatrix}.$$

We define the elements of E_{00} by

$$E_{00} = \begin{pmatrix} e_{00} & e_{01} \\ e_{10} & e_{11} \end{pmatrix},$$

which gives

$$(|e_{00}|^2 + |e_{01}|^2) + (|e_{10}|^2 + |e_{11}|^2)$$
$$= \lambda^{\vec{R}_{n-3}}(|e_{00}|^2 + |e_{01}|^2) + \frac{1}{\lambda^{\vec{R}_{n-3}}}(|e_{10}|^2 + |e_{11}|^2), \tag{122}$$

implying

$$(1 - \lambda^{\vec{R}_{n-3}})(|e_{00}|^2 + |e_{01}|^2) = (\frac{1}{\lambda^{\vec{R}_{n-3}}} - 1)(|e_{10}|^2 + |e_{11}|^2) \tag{123}$$

which is equivalent to

$$\lambda^{\vec{R}_{n-3}}(|e_{00}|^2 + |e_{01}|^2) = (|e_{10}|^2 + |e_{11}|^2). \tag{124}$$

For $(k,l) = (0,1)$ and $(k',l') = (1,1)$, we perform a similar calculation and obtain

$$\lambda^{\vec{R}_{n-3}}(\mu^{\vec{R}_{n-3}}|e_{00}|^2 + \frac{1}{\mu^{\vec{R}_{n-3}}}|e_{01}|^2)$$
$$= (\mu^{\vec{R}_{n-3}}|e_{10}|^2 + \frac{1}{\mu^{\vec{R}_{n-3}}}|e_{11}|^2). \tag{125}$$

For $(k,l) = (0,0)$ and $(k',l') = (0,1)$, Eqs. (51), (52), (53) and the cyclic property of trace imply

$$\mathrm{Tr}\, E_{00}^{\dagger} E_{00} = \mathrm{Tr} \begin{pmatrix} \sqrt{\mu^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\mu^{\vec{R}_{n-3}}}} \end{pmatrix}$$
$$\cdot E_{00}^{\dagger} E_{00} \cdot \begin{pmatrix} \sqrt{\mu^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\mu^{\vec{R}_{n-3}}}} \end{pmatrix},$$

from which we obtain

$$(|e_{00}|^2 + |e_{10}|^2) + (|e_{01}|^2 + |e_{11}|^2)$$
$$= \mu^{\vec{R}_{n-3}}(|e_{00}|^2 + |e_{10}|^2) + \frac{1}{\mu^{\vec{R}_{n-3}}}(|e_{01}|^2 + |e_{11}|^2)$$

that is equivalent to

$$\mu^{\vec{R}_{n-3}}(|e_{00}|^2 + |e_{10}|^2) = (|e_{01}|^2 + |e_{11}|^2). \tag{126}$$

For $(k,l) = (1,0)$ and $(k',l') = (1,1)$, we apply similar calculation, resulting in

$$\mu^{\vec{R}_{n-3}}(\lambda^{\vec{R}_{n-3}}|e_{00}|^2 + \frac{1}{\lambda^{\vec{R}_{n-3}}}|e_{10}|^2)$$
$$= (\lambda^{\vec{R}_{n-3}}|e_{01}|^2 + \frac{1}{\lambda^{\vec{R}_{n-3}}}|e_{11}|^2). \quad (127)$$

Multiplying Eq. (127) by $\lambda^{\vec{R}_{n-3}}$ and subtracting it from Eq. (126), we obtain

$$|e_{01}|^2 = \mu^{\vec{R}_{n-3}}|e_{00}|^2. \quad (128)$$

Multiplying Eq. (127) by $\lambda^{\vec{R}_{n-3}}$ and Eq. (126) by $(\lambda^{\vec{R}_{n-3}})^2$, and subtracting the former from the latter, we obtain

$$\mu^{\vec{R}_{n-3}}|e_{10}|^2 = |e_{11}|^2. \quad (129)$$

Using Eqs. (124), (128) , and (129), we have

$$\lambda^{\vec{R}_{n-3}}|e_{00}|^2 = |e_{10}|^2. \quad (130)$$

Therefore, we conclude from Eqs. (128), (129), and (130) that

$$E_{00} = |e_{00}|^2 \cdot \begin{pmatrix} e^{iw} & \sqrt{\mu^{\vec{R}_{n-3}}}e^{ix} \\ \sqrt{\lambda^{\vec{R}_{n-3}}}e^{iy} & \sqrt{\lambda^{\vec{R}_{n-3}}\mu^{\vec{R}_{n-3}}}e^{iz} \end{pmatrix},$$

for some real numbers w, x, y, and z.

Eq. (99) and the definition of $B'^{\vec{R}_{n-3}}_{00}$ and $B'^{\vec{R}_{n-3}}_{11}$ give us

$$E_{01}E_{01}^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\delta^{\vec{R}_{n-3}}} \end{pmatrix} E_{00}E_{00}^\dagger \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta^{\vec{R}_{n-3}}} \end{pmatrix}.$$

Comparing the $(0,1)$-element of the two sides, we have

$$\mu^{\vec{R}_{n-3}}\sqrt{\lambda^{\vec{R}_{n-3}}}e^{i(w-y)} + \sqrt{\lambda^{\vec{R}_{n-3}}}e^{i(x-z)}$$
$$= e^{i\delta^{\vec{R}_{n-3}}}(\sqrt{\lambda^{\vec{R}_{n-3}}}e^{i(w-y)} + \mu^{\vec{R}_{n-3}}\sqrt{\lambda^{\vec{R}_{n-3}}}e^{i(x-z)}).$$

Defining $\Delta' = -w+x+y-z$, the last equation is equivalent to

$$e^{i\delta^{\vec{R}_{n-3}}} = \frac{1 + \mu^{\vec{R}_{n-3}}e^{i\Delta'}}{\mu^{\vec{R}_{n-3}} + e^{i\Delta'}}.$$

Using Eq. (97), we have

$$\frac{\lambda^{\vec{R}_{n-3}} - e^{i\theta}}{\lambda^{\vec{R}_{n-3}}e^{i\theta} - 1} = \frac{1 + \mu^{\vec{R}_{n-3}}e^{i\Delta'}}{\mu^{\vec{R}_{n-3}} + e^{i\Delta'}}.$$

It can be easily checked that this equation is equivalent to

$$\frac{\mu^{\vec{R}_{n-3}} - e^{i\theta}}{\mu^{\vec{R}_{n-3}}e^{i\theta} - 1} = \frac{1 + \lambda^{\vec{R}_{n-3}}e^{i\Delta'}}{\lambda^{\vec{R}_{n-3}} + e^{i\Delta'}}.$$

The denominator and the numerator of the left hand side have the same magnitude, implying that there exists $\delta'^{\vec{R}_{n-3}}$ such that

$$\frac{\mu^{\vec{R}_{n-3}} - e^{i\theta}}{\mu^{\vec{R}_{n-3}}e^{i\theta} - 1} = e^{i\delta'^{\vec{R}_{n-3}}}. \quad (131)$$

It can be shown that ${}^tE_{00}E_{00}^*$ and ${}^tE_{10}E_{10}^*$ satisfy

$${}^tE_{10}E_{10}^* = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\delta'^{\vec{R}_{n-3}}} \end{pmatrix} {}^tE_{00}E_{00}^* \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta'^{\vec{R}_{n-3}}} \end{pmatrix}, \quad (132)$$

which can be seen as follows. First, we observe that

$${}^tE_{00}E_{00}^* = \begin{pmatrix} W_{00} & W_{01} \\ W_{10} & W_{11} \end{pmatrix} \quad (133)$$

and

$${}^tE_{10}E_{10}^* = \begin{pmatrix} W_{00} & W'_{01} \\ W'_{10} & W_{11} \end{pmatrix} \quad (134)$$

where the elements W_{kl} and W'_{kl} are given by

$$W_{00} = 1 + \lambda^{\vec{R}_{n-3}},$$
$$W_{01} = \sqrt{\mu^{\vec{R}_{n-3}}}\left(e^{i(w-x)} + \lambda^{\vec{R}_{n-3}}e^{i(y-z)}\right),$$
$$W_{10} = \sqrt{\mu^{\vec{R}_{n-3}}}\left(e^{-i(w-x)} + \lambda^{\vec{R}_{n-3}}e^{-i(y-z)}\right),$$
$$W_{11} = \mu^{\vec{R}_{n-3}}(1 + \lambda^{\vec{R}_{n-3}}),$$
$$W'_{01} = \sqrt{\mu^{\vec{R}_{n-3}}}\left(\lambda^{\vec{R}_{n-3}}e^{i(w-x)} + e^{i(y-z)}\right),$$
$$W'_{10} = \sqrt{\mu^{\vec{R}_{n-3}}}\left(\lambda^{\vec{R}_{n-3}}e^{-i(w-x)} + e^{-i(y-z)}\right).$$

Now,

$$\lambda^{\vec{R}_{n-3}}\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(w-x)} + \sqrt{\mu^{\vec{R}_{n-3}}}e^{i(y-z)}$$
$$= (\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(w-x)} + \lambda^{\vec{R}_{n-3}}\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(y-z)})$$
$$\times \frac{\lambda^{\vec{R}_{n-3}}\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(w-x)} + \sqrt{\mu^{\vec{R}_{n-3}}}e^{i(y-z)}}{\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(w-x)} + \lambda^{\vec{R}_{n-3}}\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(y-z)}}$$
$$= (\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(w-x)} + \lambda^{\vec{R}_{n-3}}\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(y-z)})$$
$$\times \frac{\mu^{\vec{R}_{n-3}} - e^{i\theta}}{\mu^{\vec{R}_{n-3}}e^{i\theta} - 1}$$
$$= (\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(w-x)} + \lambda^{\vec{R}_{n-3}}\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(y-z)}) \times e^{i\delta'^{\vec{R}_{n-3}}},$$

where the last equality follows from Eq. (131). Therefore, Eq. (132) holds.

Finally, using Eq. (121) we have

$$
{}^{t}E_{kl}E_{kl}^{*} = \begin{pmatrix} \sqrt{\mu^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\mu^{\vec{R}_{n-3}}}} \end{pmatrix}^{l} \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\delta'^{\vec{R}_{n-3}}} \end{pmatrix}^{k}
$$
$$
\times {}^{t}E_{00}E_{00}^{*} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta'^{\vec{R}_{n-3}}} \end{pmatrix}^{k} \begin{pmatrix} \sqrt{\mu^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\mu^{\vec{R}_{n-3}}}} \end{pmatrix}^{l}
$$

and

$$
\mu^{\vec{R}_{n-3}} + e^{-i\delta'^{\vec{R}_{n-3}}} = e^{i\theta}(1 + \mu^{\vec{R}_{n-3}}e^{-i\delta'^{\vec{R}_{n-3}}}),
$$

which follows directly from Eq. (131).

Using Claim 1 with Eqs. (117) and (118), we prove that, for the case $\lambda^{\vec{R}_{n-3}} \neq 1$, Eq. (112) holds. On the other hand, using Claim 1 with Eqs. (12), (83), (85), (132), we see that Eq. (111) holds. Finally, because

$$
\left| \frac{2\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(x-w)}}{1+\lambda^{\vec{R}_{n-3}}} + \frac{2\lambda^{\vec{R}_{n-3}}\sqrt{\mu^{\vec{R}_{n-3}}}e^{i(z-y)}}{1+\lambda^{\vec{R}_{n-3}}} \right| \leq 2\sqrt{\mu^{\vec{R}_{n-3}}},
$$

there exist phase factors $e^{i\varphi_0}$ and $e^{i\varphi_1}$ such that Eq. (114) holds. This completes the proof of the lemma for the case $\lambda^{\vec{R}_{n-3}} \neq 1$.

Next, let us assume $\lambda^{\vec{R}_{n-3}} = 1$. In this case, we have

$$
\tilde{A}_{00}^{\vec{R}_{n-3}}X^{t}B_{00}^{\vec{R}_{n-3}} = V^{\vec{R}_{n-3}} \begin{pmatrix} \sqrt{e_0^{\vec{R}_{n-3}}} & 0 \\ 0 & \sqrt{f_0^{\vec{R}_{n-3}}} \end{pmatrix} W_0^{\vec{R}_{n-3}*}
$$
(135)

and

$$
\tilde{A}_{00}^{\vec{R}_{n-3}}X^{t}B_{11}^{\vec{R}_{n-3}}
$$
$$
= \tilde{A}_{00}^{\vec{R}_{n-3}}X^{t}B_{00}^{\vec{R}_{n-3}}\cdot{}^{t}W_0^{\vec{R}_{n-3}} \begin{pmatrix} \sqrt{\mu^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\mu^{\vec{R}_{n-3}}}} \end{pmatrix} W_1^{\vec{R}_{n-3}*},
$$
(136)

where $W_0^{\vec{R}_{n-3}}$ and $W_1^{\vec{R}_{n-3}}$ are some unitary operators and $\mu^{\vec{R}_{n-3}} = f_0^{\vec{R}_{n-3}}/e_0^{\vec{R}_{n-3}}$, which is well defined because $B_{00}^{\vec{R}_{n-3}}$ is assumed to be full rank.

We define

$$
B'^{\vec{R}_{n-3}}_{00} = W_0^{\vec{R}_{n-3}}B_{00}^{\vec{R}_{n-3}} \tag{137}
$$
$$
B'^{\vec{R}_{n-3}}_{11} = W_1^{\vec{R}_{n-3}}B_{11}^{\vec{R}_{n-3}}, \tag{138}
$$

which together with Eq. (136) give us

$$
B'^{\vec{R}_{n-3}}_{11} = \begin{pmatrix} \sqrt{\mu^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\mu^{\vec{R}_{n-3}}}} \end{pmatrix} B'^{\vec{R}_{n-3}}_{00} \tag{139}
$$

and

$$
B'^{\vec{R}_{n-3}\dagger}_{ll}B'^{\vec{R}_{n-3}}_{ll} = B_{ll}^{\vec{R}_{n-3}\dagger}B_{ll}^{\vec{R}_{n-3}}. \tag{140}
$$

Using Claim 1 with Eqs. (139) and (140), we prove that, for the case $\lambda^{\vec{R}_{n-3}} = 1$, Eq. (112) holds.

We also define

$$
E_{kl}^{\vec{R}_{n-3}} = V^{\vec{R}_{n-3}\dagger}\tilde{A}_{kk}^{\vec{R}_{n-3}}X^{t}B'^{\vec{R}_{n-3}}_{ll}.
$$

It is easy to see that

$$
{}^{t}E_{10}E_{10}^{*} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\delta'^{\vec{R}_{n-3}}} \end{pmatrix} {}^{t}E_{00}E_{00}^{*} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta'^{\vec{R}_{n-3}}} \end{pmatrix} \tag{141}
$$

for any $e^{i\delta'^{\vec{R}_{n-3}}}$, but we choose $e^{i\delta'^{\vec{R}_{n-3}}}$ so that

$$
\mu^{\vec{R}_{n-3}} + e^{-i\delta'^{\vec{R}_{n-3}}} = e^{-i\theta}(1 + \mu^{\vec{R}_{n-3}}e^{-i\delta'^{\vec{R}_{n-3}}}).
$$

Using Claim 1 with Eqs. (12), (83), (85), (140), and (141), we see that, for the case $\lambda^{\vec{R}_{n-3}} = 1$, Eq. (111) holds. Finally, it suffices to choose

$$
e^{i\varphi_0} = 1 \text{ and } e^{i\varphi_1} = -1
$$

for Eq. (114).

$\square$

In Ref. [10], an algorithm is presented to construct a measurement operation such that an accumulated operator T 'splits' into T' and T'', where

$$
T^{\dagger}T = T'^{\dagger}T' + T''^{\dagger}T''. \tag{142}
$$

Therefore, we can find a two-outcome measurement $\{M'^{(r_{n-2}|\vec{R}_{n-3})}\}_{r_{n-2}=0,1}$ such that

$$
M'^{(r_{n-2}|\vec{R}_{n-3})}A^{\vec{R}_{n-3}} = \sqrt{\frac{|e_{00}|^2(1+\mu^{\vec{R}_{n-3}})}{2}}
$$
$$
\times \Big\{ |0\rangle\langle0| \otimes (\langle0| + \sqrt{\mu^{\vec{R}_{n-3}}}e^{i\varphi_{r_{n-2}}}\langle1|)
$$
$$
+ |1\rangle\langle1| \otimes (\langle0| + \sqrt{\mu^{\vec{R}_{n-3}}}e^{i(\varphi_{r_{n-2}}-\delta'^{\vec{R}_{n-3}})}\langle1|) \Big\}
$$
$$
\times \Big[I \otimes {}^{t}(B'^{\vec{R}_{n-3}*}X)^{-1} \Big]. \tag{143}
$$

Bob's new measurement operation $\{K'^{(r_{n-1}|\vec{R}_{n-2})}\}_{r_{n-1}=0,1}$ is given by

$$
K^{(r_{n-1}|\vec{R}_{n-2})} = (|0\rangle_{B,\text{in}}\langle0| \otimes \langle r_{n-1}|_{B,\text{r}}
$$
$$
+ |1\rangle_{B,\text{in}}\langle1| \otimes \langle r_{n-1}|_{B,\text{r}}e^{i\varphi_{r_{n-2}}}\cdot u'^{\vec{R}_{n-3}\dagger}) \cdot U_B^{\vec{R}_{n-3}\dagger},
$$

where $u'^{\vec{R}_{n-3}\dagger}$ is a unitary operator that satisfies

$$
\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\delta'\vec{R}_{n-3}} \end{pmatrix}^k \times \begin{pmatrix} \sqrt{\mu^{\vec{R}_{n-3}}} & 0 \\ 0 & \frac{1}{\sqrt{\mu^{\vec{R}_{n-3}}}} \end{pmatrix}^l
$$

$$
\times (|0\rangle_{B,r} + \sqrt{\mu^{\vec{R}_{n-3}}} e^{i\varphi_x} |1\rangle_{B,r}) =
$$

$$
\mathcal{E}_{kl}(u'^{\vec{R}_{n-3}})^l \times \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\delta'\vec{R}_{n-3}} \end{pmatrix}^k (|0\rangle_{B,r} + \sqrt{\mu^{\vec{R}_{n-3}}} e^{i\varphi_x} |1\rangle_{B,r}),
$$

$$(144)$$

whose existence is guaranteed by Eq. (113) and Claim 2.

Alice's final measurement operation $\{M'^{(r_n|\vec{R}_{n-1})}\}_{r_n}\}$ is now given by

$$
\{M'^{(r_n|\vec{R}_{n-2},0)}\} = \{\mathbb{I}_{A,\mathrm{in}}\} \tag{145}
$$

$$
\{M'^{(r_n|\vec{R}_{n-2},1)}\} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta'\vec{R}_{n-3}} \end{pmatrix}_{A,\mathrm{in}} . \tag{146}
$$

This completes the construction of the new measurements required in Lemma 3.

Proof of Lemma 4

Finally, it can be seen that Eqs. (16), (48), (83), and (104) imply Eq. (20), proving Lemma 4.